UNITED STATES DISTRICT COURT

FOR THE WESTERN DISTRICT OF WASHINGTON

JACK PRECOUR, WILLIAM CAPTAIN REED, CESAR LOPEZ, TOMASINA ENOCH, MARSHALL P. JONES, JR., and CORNELIA CLAY FULGHUM, Individually and on Behalf of All Others Similarly Situated,

Plaintiffs,

v.

T-MOBILE USA, INC.

Defendant.

Case No.:

CLASS ACTION COMPLAINT FOR:

(1) Negligence
(2) Negligence Per Se
(3) Gross Negligence
(4) Unjust Enrichment
(5) Breach of Implied Contract
(6) Declaratory and Injunctive Relief
(7) Violations of State Statutes

DEMAND FOR JURY TRIAL

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Plaintiffs, identified in Section II.A. below, individually and on behalf of all others similarly situated ("Plaintiffs"), bring this action against T-Mobile US, Inc., ("T-Mobile"), seeking monetary damages, restitution, and/or injunctive relief. Plaintiffs make the following allegations upon personal knowledge and on information and belief derived from, among other things, investigation by their counsel and facts that are a matter of public record.

I. NATURE OF THE ACTION

1. Plaintiffs bring this lawsuit as a result of a cybercriminal's accessing and stealing data held, but poorly protected, by the Defendant T-Mobile. After data was stolen from its servers, T-Mobile notified approximately 54 million current subscribers, prospective customers, and former subscribers that data (collectively referred to hereafter as "Private Information") pertaining to them, including their Personally Identifying Information ("PII"), had been accessed and stolen.

2. T-Mobile's servers contained Private Information of individuals, including Plaintiffs. According to the Federal Trade Commission ("FTC"), PII is "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual."[1]

3. T-Mobile is the second-largest wireless carrier and service provider in the United States, boasting 104.8 million subscribers[2]—and handsome[3] annual revenues—due to their large market share. T-Mobile requires that potential customers provide certain Private Information to become a subscriber: a customer's full name, address, social security number,

[1] *See Federal Trade Commission Privacy Impact Assessment: Redress Enforcement Database (RED)* at 3, n.3, FTC (June 2019), https://www.ftc.gov/system/files/attachments/privacy-impact-assessments/redress_enforcement_database_red_privacy_impact_assessment_june_2019.pdf.
[2] *T-Mobile US, Inc. Quarterly Financial Results*, available at https://investor.t-mobile.com/financial-performance/quarterly-results/default.aspx (last accessed Sep. 7, 2021).
[3] T-Mobile took in approximately $68.4 billion in revenues in 2020. T-Mobile US, Inc., Annual Report (Form 10-K) (hereinafter "2020 Form 10-K") at 1, available at https://www.sec.gov/Archives/edgar/data/0001283699/000128369921000039/tmus-20201231.htm (last accessed Sep. 7, 2021).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

banking information, driver's license information, and other PII are frequently and commonly required.

4. The value of this information is recognized by several different constituencies. First, the value is recognized by T-Mobile: in a recent press release regarding the data breach, T-Mobile CEO Mike Sievert acknowledged that "[k]eeping our customers' data safe is a responsibility we take incredibly seriously and preventing this type of event from happening has always been a top priority of ours. Unfortunately, this time we were not successful."[4] Second, the value is recognized by cybercriminals, who know that this type of data can be exploited for ransom payments, sold on a virulent black market for substantial sums, and used to commit identity theft. And third, the value is recognized by the individuals, themselves, whose data was stolen.

5. T-Mobile identifies itself as the "Un-carrier" in a bid to "change the game" with regard to providing mobile and wireless service to its customers.[5] T-Mobile markets itself as the major alternative to other American wireless networks, and touts its "re-invention of the old, broken customer service model" and its "100% customer commitment" as hallmarks of what make its service distinguishable.[6]

6. Millions of individuals have shared their most valuable Private Information with T-Mobile based on the ordinary, reasonable understanding that their information would be handled and maintained with appropriate safety standards.

7. Despite T-Mobile's representations that it is "customer obsessed" and assurances that T-Mobile takes proper steps to protect the Private Information that T-Mobile requires its customers to provide in order to become subscribers, its security program was woefully inadequate. T-Mobile's unsound, vulnerable systems containing valuable data were an open

[4] Mike Sievert, "The Cyberattack Against T-Mobile and Our Customers: What happened, and what we are doing about it." (hereinafter "Sievert Statement"), available at https://www.t-mobile.com/news/network/cyberattack-against-tmobile-and-our-customers (last accessed Sep. 7, 2021).
[5] "Un-Carrier History", available at https://www.t-mobile.com/our-story/un-carrier-history (last accessed Sep. 7, 2021).
[6] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

invitation for an intrusion and extraction of data by cybercriminals, who sought to exploit the valuable nature of the information.

8. The release, disclosure, and publication of a person's sensitive, private data can be devastating. Not only is it an intrusion of privacy and a loss of control, but it is also a harbinger of identity theft: for victims of a data breach, the risk of identity theft more than quadruples.[7] A data breach can have grave consequences for victims for many years after the actual date of the breach—with the obtained information, identity thieves can wreak many forms of havoc: open new financial accounts, take out loans, obtain medical services, obtain government benefits, or obtain driver's licenses in the victims' names, forcing victims to maintain a constant vigilance over the potential misuse of their information.

9. T-Mobile was keenly aware of the risks of cyberattacks and breaches of its customers' confidential data. It knew of the risk because T-Mobile had suffered a string of cybersecurity incidents in the preceding three years.[8] Despite indications that T-Mobile's network security was hopelessly inadequate, T-Mobile failed to take the proper steps to defend its network from even the most rudimentary of attacks.

10. T-Mobile also showed that it knew of the risk it faced by virtue of its own representations. In its Annual Report filed with the SEC, T-Mobile stated that "We could be harmed by data loss or other security breaches" and that T-Mobile's "business involves the receipt, storage and transmission of our customers' confidential information." T-Mobile acknowledged in that filing that "[u]nauthorized access to Confidential Information may be difficult to anticipate, detect, or prevent" and that T-Mobile is "subject to the threat of unauthorized access or disclosure of Confidential Information" by a host of different threats, including state-sponsored hackers, malicious bad actors, employees, errors or breaches by third-

[7] Dave Maxfield & Bill Latham, *Data Breaches: Perspectives from Both Sides of the Wall*, S.C. Law (May 2014).

[8] Cammy Pedroja, *T-Mobile Hacked for 5th Time in 4 Years in Latest Breach; Nearly 50 Million Affected*, NEWSWEEK, available at https://www.newsweek.com/t-mobile-hacked-5th-time-4-years-latest-breach-nearly-50-million-affected-1620710 (last accessed Sep. 7, 2021).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

party suppliers, or others that might compromise the confidentiality and integrity of their customers Private Information.[9]

11. T-Mobile likewise was aware of the significant risk of cyberattacks, stating that "future cyber-attacks, data breaches, or security incidents may have a material adverse effect on our business, financial condition and operating results."[10] In that same document, T-Mobile also acknowledged its obligation to continually re-evaluate and revise its data, network, and cybersecurity practices to address an "ever-evolving threat landscape."[11]

12. Nonetheless, T-Mobile failed to detect and stop the theft of the Private Information of millions of potential customers, current subscribers, and previous customers it held insecurely on its servers.

13. Unlike in other most data breach events, one of the cybercriminals responsible for this breach has publicly claimed responsibility. John Binns, a 21-year-old American who lives in Turkey, detailed the tactics he used to accomplish the breach, stating in an interview with the Wall Street Journal that he accessed one of T-Mobile's unprotected routers and weak spots in the company's internet addresses that gave him access to over 100 servers.[12]

14. While Mr. Binns accessed T-Mobile's sensitive systems as early as July 28, 2021 (and began lifting troves of data on August 4, 2021) T-Mobile did not report the data breach until August 16, 2021. During that time, Mr. Binns was able to access the PII of tens of millions of T-Mobile customers, and even people who were only potential customers of T-Mobile, or had not been customers of T-Mobile for years.

15. The exposure of this data is not potential or hypothetical: on August 13, 2021, the security research firm Unit221B LLC reported to T-Mobile that an account was attempting

---

[9] 2020 Form 10-K, at 12.
[10] *Id.*
[11] *Id.*
[12] Drew Fitzgerald and Robert McMillan, *T-Mobile Hacker Who Stole Data on 50 Million Customers: 'Their Security Is Awful'*, THE WALL STREET JOURNAL, Aug. 27, 2021, available at https://www.wsj.com/articles/t-mobile-hacker-who-stole-data-on-50-million-customers-their-security-is-awful-11629985105 (last accessed Sep. 7, 2021).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

to sell T-Mobile customer data on the dark web. It was this report that brought the data breach to T-Mobile's attention in the first place.[13]

16. Despite pressure from the federal government,[14] and two previous, less successful cybersecurity attacks in 2020,[15] T-Mobile utterly failed to secure its systems.

17. The Data Breach, as described herein, was accomplished with relative ease: Mr. Binns indicated in an interview that he was able to breach T-Mobile's defenses by scanning T-Mobile's known internet addresses for weak spots using a simple tool available online to the public.

18. Despite the relatively low-tech nature of the data breach in this case, an array of personal details from T-Mobile's potential, present, and former customers was stolen, including full names, social security numbers, birth dates, IMEI and IMSI numbers used to identify individual customers' devices (such as smart phones), and driver's license numbers.

19. T-Mobile's unlawfully deficient data security and utter failure to protect against criminal cybersecurity attacks it knew it would face has injured millions of customers, potential customers, and former customers, the Plaintiffs and putative class members in this action.

20. Had T-Mobile maintained a sufficient security program, including properly monitoring its network, security, and communications, it would have discovered the cyberattack sooner or prevented it altogether. In fact, T-Mobile recently announced it has entered into "long-term partnerships" with two "industry-leading cybersecurity experts" to help take their "cybersecurity efforts to the next level."[16] Had these partnerships been forged before the data breach (only the latest in a string of five major cybersecurity incidents to happen to T-Mobile in

---

[13] *Id.*

[14] Drew Fitzgerald, *T-Mobile Vows to Fight FCC Fines for Location Sharing*, THE WALL STREET JOURNAL, Feb. 28, 2020, available at https://www.wsj.com/articles/t-mobile-vows-to-fight-fcc-fines-for-location-sharing-11582921450?mod=article_inline (last accessed Sep. 7, 2021).

[15] https://www.t-mobile.com/responsibility/consumer-info/pii-notice; https://www.t-mobile.com/responsibility/consumer-info/security-incident.

[16] Sievert Statement.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

the last three years), this incident would not have happened, and Plaintiffs' Private Information would not have been accessed.

21. Plaintiffs' Private Information has been compromised and disclosed to unauthorized third parties because of T-Mobile's negligent and unlawful conduct—the PII that T-Mobile collected and maintained is now in the hands of cybercriminals. T-Mobile's notices to its present, potential and former customers advised that class members should remain aware of suspicious account activity, sign up for T-Mobile's free scam-blocking protection ("Scam Shield"), change their account PINs, enroll in T-Mobile's "Account Takeover Protection" service, take further actions such as monitoring their own credit records, freeze their credit and implement fraud alerts, and notify law enforcement authorities of any suspicious activity.[17]

22. Regardless of these suggestions, Plaintiffs and millions of class members have suffered and will continue to suffer concrete and actual harm as a direct result of this Data Breach. Plaintiffs' and the class members' sensitive PII—which was entrusted to T-Mobile—was compromised and unlawfully accessed as a result of the Data Breach and made subject to unlawful use by cybercriminals.

23. As a result of the Data Breach, Plaintiffs and the class members have suffered concrete damages and are now exposed to a heightened and imminent risk of fraud, identity theft, and ransom demands for many years to come. Furthermore, Plaintiffs and class members must now and in the future closely monitor their financial accounts to guard against identity theft at their own expense. Consequently, Plaintiffs and the class members will incur ongoing out-of-pocket costs including the cost of credit monitoring services, credit freezes, credit reports, and other protective measures to deter and detect identity theft, among other expenses.

[17] "Additional Steps to Protect Yourself", available at https://www.t-mobile.com/support/account/additional-steps-to-protect-yourself?icid=MGPO_MTW_U_21DTASECRT_SVFBJIM81C0IT0Q26102 (last accessed Sep. 7, 2021).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

24. By this Complaint, Plaintiffs seek to remedy these harms on behalf of themselves and all similarly situated individuals whose Private Information was compromised and disclosed as a result of the Data Breach.

25. Accordingly, Plaintiffs bring this action against T-Mobile seeking redress for its unlawful conduct, and asserting claims for both common law and statutory damages.

II. PARTIES

A. Plaintiffs

26. Plaintiffs identified below bring this action on behalf of themselves and those similarly situated in a representative capacity for individuals across the United States. Despite knowing of the substantial cybersecurity risks it faced, T-Mobile, through its actions described herein, leaked, disbursed, and furnished Plaintiffs' valuable Private Information to unknown cybercriminals, thus causing them present, immediate, imminent, and continuing increased risk of harm.

27. As used throughout this Complaint, "Private Information" is further defined as all information exposed by the Data Breach, including all or any part or combination of name, address, birth date, SSN, PHI, driver's license information (including license number, state, home address, dates of issuance or expiration), telephone number, email address, tax identification number, credit card number, or dispute documents with PII (such as images of government-issued identifications).

28. Based upon counsel's investigation, and upon information and belief, residents and citizens of all States not specifically enumerated below were affected by the Data Breach. The Plaintiffs identified below in this Complaint are pursuing claims on their own behalf, and on behalf of the citizens and residents of California, North Carolina, Pennsylvania, Texas, and Virginia.

CALIFORNIA

29. Plaintiff **Diego Quintanilla** ("Quintanilla") is a resident and citizen of California. Plaintiff Quintanilla is acting on his own behalf and on behalf of others similarly

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

situated. T-Mobile obtained and continues to maintain Plaintiff Quintanilla's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Quintanilla would not have entrusted his Private Information to T-Mobile had he known that T-Mobile had failed to maintain adequate data security for his Private Information. Plaintiff Quintanilla's Private Information was compromised and disclosed as a result of the Data Breach.

30. Plaintiff Quintanilla became a T-Mobile customer prior to the data breach alleged in this Complaint.

31. Plaintiff Quintanilla was a contract subscriber to T-Mobile at the time of the Data Breach, and first became a T-Mobile contract subscriber in 1998.

32. Plaintiff Quintanilla became a contract subscriber when he opened up a T-Mobile account in a store.

33. Plaintiff Quintanilla was required to provide his Private Information to T-Mobile as a condition of becoming a T-Mobile subscriber and customer.

34. Shortly after the Data Breach was announced, Plaintiff Quintanilla received an alert on his phone through his T-Mobile app. That notification indicated to him that there had been a data breach, and that his Private Information may have been improperly accessed and/or obtained by unauthorized third parties. This notice only indicated that Plaintiff Quintanilla's private information had been accessed, but did not identify which information may have been compromised as a result of the Data Breach.

35. This notice further indicated that the Data Breach did not involve the exposure of debit or credit card information, or that any passwords, postpaid PIN numbers, or financial or payment information was compromised. However, because T-Mobile has not offered much in the way of specifics as to each customer, it is at this time unclear how much Private Information of Plaintiff Quintanilla's was exposed due to T-Mobile's conduct.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

36. Since the Data Breach, Plaintiff Quintanilla has noticed an uptick in phishing, scam, and spam emails and texts, often skillfully mocked up to appear to be genuine, legitimate communications from T-Mobile itself.

37. As a result of the Data Breach, Plaintiff Quintanilla has made reasonable efforts to mitigate its impact after receiving the notification text and email, including but not limited to: researching the Data Breach and T-Mobile; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud, and engaging in the free credit monitoring service from McAfee offered to him by T-Mobile.

38. Plaintiff Quintanilla has already spent approximately 5 hours reviewing credit monitoring reports and/or checking account statements, and Plaintiff Quintanilla expects to spend at least two hours per month reviewing these reports and statements for the foreseeable future. These expenditures reflect the loss of valuable time Plaintiff Precour otherwise would have spent on other activities, including but not limited to work and/or recreation.

39. Plaintiff Quintanilla suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PI, a form of property that T-Mobile obtained from Plaintiff Quintanilla; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

40. As a result of the Data Breach, Plaintiff Quintanilla anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Quintanilla will continue to be at increased risk of identity theft and fraud for years to come.

41. Plaintiff **William Captain Reed** ("Reed") is a resident and citizen of California. Plaintiff Reed is acting on his own behalf and on behalf of others similarly situated. T-Mobile obtained and continues to maintain Plaintiff Reed's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Reed would not have entrusted his Private Information to T-Mobile had he known that T-

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Mobile had failed to maintain adequate data security for his Private Information. Plaintiff Reed's Private Information was compromised and disclosed as a result of the Data Breach.

42. Plaintiff Reed became a T-Mobile customer prior to the data breach alleged in this Complaint.

43. Plaintiff Reed was a contract subscriber to T-Mobile at the time of the Data Breach.

44. Plaintiff Reed was required to provide his Private Information to T-Mobile as a condition of becoming a T-Mobile subscriber and customer.

45. Shortly after the Data Breach was announced, Plaintiff Reed called T-Mobile to ask a question about his most recent bill. During that conversation, it was indicated to him that there had been a data breach, and that his Private Information may have been improperly accessed and/or obtained by unauthorized third parties. This notice only indicated that Plaintiff Reed's private information had been accessed, but did not identify which information may have been compromised as a result of the Data Breach.

46. This notice further indicated that the Data Breach did not involve the exposure of debit or credit card information, or that any passwords, postpaid PIN numbers, or financial or payment information was compromised. However, because T-Mobile has not offered much in the way of specifics as to each customer, it is at this time unclear how much Private Information of Plaintiff Reed's was exposed due to T-Mobile's conduct.

47. As a result of the Data Breach, Plaintiff Reed has made reasonable efforts to mitigate its impact after receiving the notification text and email, including but not limited to: researching the Data Breach and T-Mobile; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud, and engaging in the free credit monitoring service from McAfee offered to him by T-Mobile.

48. After enrolling in the McAfee service, Plaintiff Reed received an additional notice that his email address had been found in a scan of the dark web.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

49. Plaintiff Reed has already spent approximately 5 hours reviewing credit monitoring reports and/or checking account statements, and Plaintiff Reed expects to spend at least two hours per month reviewing these reports and statements for the foreseeable future. These expenditures reflect the loss of valuable time Plaintiff Precour otherwise would have spent on other activities, including but not limited to work and/or recreation.

50. Plaintiff Reed suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PI, a form of property that T-Mobile obtained from Plaintiff Reed; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

51. As a result of the Data Breach, Plaintiff Reed anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Reed will continue to be at increased risk of identity theft and fraud for years to come.

NORTH CAROLINA

52. Plaintiff Cesar Lopez ("Lopez") is a resident and citizen of North Carolina. Plaintiff Lopez is acting on his own behalf and on behalf of others similarly situated. T-Mobile obtained and continues to maintain Plaintiff Lopez's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Lopez would not have entrusted his Private Information to T-Mobile had he known that T-Mobile had failed to maintain adequate data security for his Private Information. Plaintiff Silverman's Private Information was compromised and disclosed as a result of the Data Breach.

53. Plaintiff Lopez became a T-Mobile customer prior to the data breach alleged in this Complaint. Plaintiff Lopez was previously an AT&T contract subscriber, and became a T-Mobile contract subscriber because he was interested in checking out what AT&T's competition could do for him.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

54. Plaintiff Lopez was a contract subscriber to T-Mobile at the time of the Data Breach.

55. Plaintiff Lopez was required to provide his Private Information to T-Mobile as a condition of becoming a T-Mobile subscriber and customer.

56. Shortly after the Data Breach was announced, Plaintiff Lopez was informed of the Data Breach by a friend who runs a YouTube channel which focuses on news and events connected to wireless networks. Thereafter, Plaintiff Lopez contacted T-Mobile, and it was indicated to him that there had been a data breach, and that his Private Information may have been improperly accessed and/or obtained by unauthorized third parties. This notice only indicated that Plaintiff Lopez's private information had been accessed, but did not identify which information may have been compromised as a result of the Data Breach.

57. This notice further indicated that the Data Breach did not involve the exposure of debit or credit card information, or that any passwords, postpaid PIN numbers, or financial or payment information was compromised. However, because T-Mobile has not offered much in the way of specifics as to each customer, it is at this time unclear how much Private Information of Plaintiff Lopez's was exposed due to T-Mobile's conduct.

58. As a result of the Data Breach, Plaintiff Lopez has made reasonable efforts to mitigate its impact after receiving the notification text and email, including but not limited to: researching the Data Breach and T-Mobile; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud; and freezing his credit.

59. Plaintiff Lopez has already received notice that someone attempted to purchase a vehicle using his name and Private Information.

60. Plaintiff Lopez has already spent approximately 5 hours reviewing credit monitoring reports and/or checking account statements, and Plaintiff Lopez expects to spend at least two hours per month reviewing these reports and statements for the foreseeable future.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

These expenditures reflect the loss of valuable time Plaintiff Precour otherwise would have spent on other activities, including but not limited to work and/or recreation.

61. Plaintiff Lopez suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PI, a form of property that T-Mobile obtained from Plaintiff Lopez; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

62. As a result of the Data Breach, Plaintiff Lopez anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Lopez will continue to be at increased risk of identity theft and fraud for years to come.

PENNSYLVANIA

63. Plaintiff **Tomasina Enoch** ("Enoch") is a resident and citizen of Pennsylvania. Plaintiff Enoch is acting on her own behalf and on behalf of others similarly situated. T-Mobile obtained and continues to maintain Plaintiff Enoch's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Enoch would not have entrusted her Private Information to T-Mobile had she known that T-Mobile had failed to maintain adequate data security for her Private Information. Plaintiff Enoch's Private Information was compromised and disclosed as a result of the Data Breach.

64. Plaintiff Enoch became a T-Mobile subscriber approximately three months before the Data Breach was announced.

65. Plaintiff Enoch previously had service through AT&T, and switched to T-Mobile in part because of T-Mobile's deceptive marketing.

66. Plaintiff Enoch was required to provide her Private Information to T-Mobile as a condition of becoming a T-Mobile subscriber and customer.

67. On or around August 19, 2021, Plaintiff Enoch received an email and a text message from T-Mobile that there had been a data breach, and that her Private Information may

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

have been improperly accessed and/or obtained by unauthorized third parties. This initial notice only indicated that Plaintiff Enoch's private information had been accessed, but did not identify which information may have been compromised as a result of the Data Breach.

68. This notice further indicated that the Data Breach did not involve the exposure of debit or credit card information, or that any passwords, postpaid PIN numbers, or financial or payment information was compromised. However, because T-Mobile has not offered much in the way of specifics as to each customer, it is at this time unclear how much Private Information of Plaintiff Enoch's was exposed due to T-Mobile's conduct.

69. As a result of the Data Breach, Plaintiff Enoch has made reasonable efforts to mitigate its impact after receiving the notification text and email, including but not limited to: researching the Data Breach and T-Mobile; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud, and monitoring her accounts for fraudulent charges.

70. Plaintiff Enoch now spends at least one hour per month reviewing credit monitoring reports and/or checking account statements. To date, Plaintiff has spent at least 10 hours on these tasks, valuable time Plaintiff Precour otherwise would have spent on other activities, including but not limited to work and/or recreation.

71. Plaintiff Enoch suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PI, a form of property that T-Mobile obtained from Plaintiff Enoch; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

72. As a result of the Data Breach, Plaintiff Enoch anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Enoch will continue to be at increased risk of identity theft and fraud for years to come.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

TEXAS

73. Plaintiff **John D. Precour (**"Precour") is a resident and citizen of Texas. Plaintiff Precour is acting on his own behalf and on behalf of others similarly situated. T-Mobile obtained and continues to maintain Plaintiff Precour's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Precour would not have entrusted his Private Information to T-Mobile had he known that T-Mobile had failed to maintain adequate data security for his Private Information. Plaintiff Precour's Private Information was compromised and disclosed as a result of the Data Breach.

74. Plaintiff Precour was required to provide his Private Information to T-Mobile as a condition of becoming a T-Mobile subscriber and customer.

75. On or around August 19, 2021, Plaintiff Precour received a notice from T-Mobile that there had been a data breach, and that his Private Information may have been improperly accessed and/or obtained by unauthorized third parties. This initial notice only indicated that Plaintiff Precour's private information had been accessed, but did not identify which information may have been compromised as a result of the Data Breach.

76. This notice further indicated that the Data Breach did not involve the exposure of debit or credit card information, or that any passwords, postpaid PIN numbers, or financial or payment information was compromised. However, because T-Mobile has not offered much in the way of specifics as to each customer, it is at this time unclear how much Private Information of Plaintiff Precour's was exposed due to T-Mobile's conduct.

77. As a result of the Data Breach, Plaintiff Precour made reasonable efforts to mitigate its impact after receiving the notification text, including but not limited to: researching the Data Breach and T-Mobile; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. In addition, as a result of the Data Breach, Plaintiff Precour also attempted to enroll in the McAfee's ID Theft Protection Service offered by T-Mobile to its affected customers, but was told upon calling them that they would

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

be in touch in a couple of days, and generally did not seem to appreciate that time was of the essence.

78. Plaintiff Precour now spends at least one hour per month reviewing credit monitoring reports and/or checking account statements. To date, Plaintiff has spent at least 10 hours on these tasks, valuable time Plaintiff Precour otherwise would have spent on other activities, including but not limited to work and/or recreation.

79. Plaintiff Precour suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PI, a form of property that T-Mobile obtained from Plaintiff Precour; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

80. As a result of the Data Breach, Plaintiff Precour anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Precour will continue to be at increased risk of identity theft and fraud for years to come.

VIRGINIA

81. Plaintiff **Marshall P. Jones, Jr. (**"Jones") is a resident and citizen of Virginia. Plaintiff Jones is acting on his own behalf and on behalf of others similarly situated. T-Mobile obtained and continues to maintain Plaintiff Jones's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Jones would not have entrusted his Private Information to T-Mobile had he known that T-Mobile had failed to maintain adequate data security for his Private Information. Plaintiff Jones's Private Information was compromised and disclosed as a result of the Data Breach.

82. Plaintiff Jones was required to provide his Private Information to T-Mobile as a condition of becoming a T-Mobile subscriber and customer.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

83. Plaintiff Jones became a T-Mobile subscriber after Sprint was acquired by T-Mobile. He was a Sprint subscriber for approximately 20 years prior to being ported over to T-Mobile.

84. On or around August 19, 2021, Plaintiff Jones saw a media report on television regarding the Data Breach.

85. Thereafter, Plaintiff Jones received an email notice from T-Mobile that there had been a data breach, and that his Private Information may have been improperly accessed and/or obtained by unauthorized third parties. This initial notice only indicated that Plaintiff Jones's private information had been accessed, but did not identify which information may have been compromised as a result of the Data Breach.

86. This notice further indicated that the Data Breach did not involve the exposure of debit or credit card information, or that any passwords, postpaid PIN numbers, or financial or payment information was compromised. However, because T-Mobile has not offered much in the way of specifics as to each customer, it is at this time unclear how much Private Information of Plaintiff Jones's was exposed due to T-Mobile's conduct.

87. As a result of the Data Breach, Plaintiff Jones made reasonable efforts to mitigate its impact after receiving the notification text, including but not limited to: researching the Data Breach and T-Mobile; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud. In addition, as a result of the Data Breach, Plaintiff Jones also attempted to enroll in the McAfee's ID Theft Protection Service offered by T-Mobile to its affected customers, but was unable to because he had an old, inactive McAfee account.

88. Plaintiff Jones already had credit monitoring services through AAA and Experian Protect My ID, which he has consulted and will continue to monitor for evidence of suspicious transactions, identity theft, or fraud.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

89. Plaintiff Jones now spends at least one hour per month reviewing credit monitoring reports and/or checking account statements. To date, Plaintiff has spent at least 10 hours on these tasks, valuable time Plaintiff Jones otherwise would have spent on other activities, including but not limited to work and/or recreation.

90. Plaintiff Jones suffered actual injury from having his Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of his PI, a form of property that T-Mobile obtained from Plaintiff Jones; (b) violation of his privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

91. As a result of the Data Breach, Plaintiff Jones anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Jones will continue to be at increased risk of identity theft and fraud for years to come.

92. Plaintiff **Cornelia Clay Fulghum** ("Fulghum") is a resident and citizen of Virginia. Plaintiff Fulghum is acting on her own behalf and on behalf of others similarly situated. T-Mobile obtained and continues to maintain Plaintiff Fulghum's Private Information and has a legal duty and obligation to protect that Private Information from unauthorized access and disclosure. Plaintiff Fulghum would not have entrusted her Private Information to T-Mobile had she known that T-Mobile had failed to maintain adequate data security for her Private Information. Plaintiff Fulghum's Private Information was compromised and disclosed as a result of the Data Breach.

93. Plaintiff Fulghum is not a T-Mobile subscriber, in that she does not have a T-Mobile account in her name.

94. Plaintiff Fulghum previously had service through Sprint, under her husband's plan, which was ported to T-Mobile after T-Mobile acquired Sprint.

95. Plaintiff Fulghum at no point agreed to a service contract with T-Mobile.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

96. However, Fulghum is a member of the family plan obtained by her husband, Plaintiff Marshall Jones.

97. Plaintiff Fulghum was required to provide her Private Information to T-Mobile as a condition of becoming a T-Mobile subscriber and customer.

98. Plaintiff Fulghum has not received an email or text message notification from T-Mobile that her Private Information was implicated in the Data Breach.

99. Plaintiff Fulghum has begun receiving targeted spam and spearphising emails designed to look like they come from T-Mobile, and which request that she input certain information or follow certain links to redeem winnings or access exclusive deals.

100. This notice further indicated that the Data Breach did not involve the exposure of debit or credit card information, or that any passwords, postpaid PIN numbers, or financial or payment information was compromised. However, because T-Mobile has not offered much in the way of specifics as to each customer, it is at this time unclear how much Private Information of Plaintiff Fulghum's was exposed due to T-Mobile's conduct.

101. As a result of the Data Breach, Plaintiff Fulghum has made reasonable efforts to mitigate its impact after receiving the notification text and email, including but not limited to: researching the Data Breach and T-Mobile; reviewing credit reports and financial account statements for any indications of actual or attempted identity theft or fraud, and monitoring her accounts for fraudulent charges.

102. Plaintiff Fulghum now spends at least one hour per month reviewing credit monitoring reports and/or checking account statements. To date, Plaintiff has spent at least 10 hours on these tasks, valuable time Plaintiff Precour otherwise would have spent on other activities, including but not limited to work and/or recreation.

103. Plaintiff Fulghum suffered actual injury from having her Private Information compromised as a result of the Data Breach including, but not limited to (a) damage to and diminution in the value of her PI, a form of property that T-Mobile obtained from Plaintiff

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Fulghum; (b) violation of her privacy rights; and (c) imminent and impending injury arising from the increased risk of identity theft and fraud.

104. As a result of the Data Breach, Plaintiff Fulghum anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harms caused by the Data Breach. Plaintiff Fulghum will continue to be at increased risk of identity theft and fraud for years to come.

ALL OTHER STATES

105. Based upon counsel's investigation, and upon information and belief, residents and citizens from all other States and Territories in the United States were affected by the Data Breach. The Plaintiffs identified in this Complaint are pursuing claims on behalf of citizens and residents of all other States and Territories not specifically enumerated here.

B. Defendant

106. Defendant T-Mobile US, Inc. is a Delaware corporation with its principal place of business located at 12920 SE 38th Street. Bellevue, Washington. T-Mobile's common stock is publicly traded on the NASDAQ under the ticker symbol "TMUS." T-Mobile provides wireless services to 102.1 million postpaid and prepaid customers and generates revenue by providing affordable wireless communications services to these customers, as well as a wide selection of wireless devices and accessories.[18]

III. JURISDICTION AND VENUE

107. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1332(d)(2)(A), as modified by the Class Action Fairness Act of 2005 ("CAFA"), 28 U.S.C. § 1711, et seq., because at least one member of the Class, as defined below, is a citizen of a different state than T-Mobile, there are more than 100 members of the Class, and the aggregate amount in controversy exceeds $5,000,000, exclusive of interest and costs.

108. This Court has personal jurisdiction over this action because T-Mobile maintains its principal place of business in this District, has sufficient minimum contacts with this District

[18] 2020 Form 10-K at 5, *supra* n. 2.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

and has purposefully availed itself of the privilege of doing business in this District, such that it could reasonably foresee litigation being brought in this District. This Court also has diversity jurisdiction over this action. See 28 U.S.C. § 1332(a).

109. Venue is proper in this District under 28 U.S.C. § 1391(a) through (d) because T-Mobile's principal place of business is located in this District and a substantial part of the events or omissions giving rise to the claims occurred in, was directed to, and/or emanated from this District. Venue is also proper in this District pursuant to 28 U.S.C. § 1391(b) based on the transfer order of the Judicial Panel on Multidistrict Litigation.

IV. INTRADISTRICT ASSIGNMENT

110. Assignment to the Seattle Division is appropriate under Civil Local Rule 3(e)(1) because a substantial part of the events or omissions which gave rise to Plaintiffs' claims occurred within King County, including the location of T-Mobile's headquarters which likely served as the hub of T-Mobile decisions concerning data protection for its users.

V. STATEMENT OF FACTS

A. T-Mobile: The Unsecured Un-carrier

111. Formed in 1994 as VoiceStream Wireless PCS and having gone through numerous acquisitions and mergers over the last twenty-seven years, T-Mobile describes itself as "the Un-carrier" and America's "largest and fastest 5G network."[19] It provides "wireless communications services through a variety of service plan options" to its clients use for personal and business use.[20]

112. T-Mobile is a publicly-traded company which provides its services primarily to two "kinds" of customers: "postpaid customers," which generally include customers who are qualified to pay after receiving wireless communications services utilizing phones, wearables, or other connected devices, which include tablets and SyncUp products; and "prepaid customers," which generally include customers who pay for wireless communications services

[19] 2020 Form 10-K at 5, *supra* n. 2.
[20] *Id* at 5.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

in advance.[21] T-Mobile also recently merged with Sprint, which greatly enhanced T-Mobile's spectrum position, and integration of the spectrum network is expected to occur over the next three years.[22]

113. T-Mobile's marketing has proved to be lucrative, as T-Mobile reported that by the end of 2020 it had approximately "102.1 million postpaid and prepaid customers" and more than $64 billion in annual revenue.[23] T-Mobile's customer-focused business requires that it collect, manage, and maintain vast reserves of customer PII.

114. In the ordinary course of doing business with T-Mobile, individual customers are regularly required to provide PII that is collected, stored, maintained, and secured by T-Mobile. This PII includes one or several of the following categories of data:[24]

- Name;
- Address;
- Phone number(s);
- Email address;
- Date of birth;
- Demographic information;
- SSN;
- Driver's license numbers;
- Government identification;
- Credit card account numbers;
- Bank account numbers;
- Educational history;
- Photo identification;
- Employer information;

[21] *Id* at 6.
[22] *Id.*
[23] *Id.* at 29.
[24] *T-Mobile Privacy Notice*, T-Mobile, available at https://www.t-mobile.com/privacy-center/our-practices/privacy-policy (last accessed Sep. 7, 2021).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

- Income information;
- Device identifier information;
- Other Private Information, including passwords, places of birth, and mothers' maiden names.

115. T-Mobile collects this PII from individuals and stores it. However, in that collection and storage, T-Mobile promises to provide confidentiality and security for its customers' and potential customers' information. In its Privacy Notice,[25] T-Mobile acknowledges that its current and potential customers "trust T-Mobile to connect [them] to the world every day, and [T-Mobile is] working hard to earn a place in [their] heart[s]. A big part of that is maintaining [customer] privacy." Beyond simply acknowledging the need to protect their customers PII, T-Mobile states that it uses "administrative, technical, contractual, and physical safeguards designed to protect [customer] data while it is under [T-Mobile's] control."[26]

116. Despite these assurances, it appears that T-Mobile did not live up to its promises.

B. T-Mobile's Network is Breached

117. On or about July 28, 2021, a hacker named John Binns, potentially aided by other hackers, procured system access to T-Mobile's servers through an unprotected router.[27]

118. Over the course of the next week, Binns burrowed into T-Mobile's servers that contained personal data about the carrier's tens of millions of former and current customers, and extracted this data around August 4, 2021.[28]

119. Mr. Binns reportedly used an entry point in one of T-Mobile's data centers outside of East Wenatchee, Washington, where stored login credentials allowed him to access more than 100 of T-Mobile's servers.[29]

---

[25] *Id.*
[26] *Id.*
[27] Fitzgerald and McMillan, *infra* n. 12.
[28] *Id.*
[29] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

120. After this extraction, the security research firm Unit221B LLC reported to T-Mobile that it had identified an account that was attempting to sell T-Mobile customer data on August 13, 2021. The unidentified seller, using an underground forum, offered to sell a subset of the data containing 30 million social security numbers and driver licenses for 6 bitcoins, or approximately $270,000. The seller said they were already in the process of privately selling the rest of the data.[30]

121. Three days later, on August 16, 2021, T-Mobile publicly acknowledged it was investigating a potential breach.[31]

122. On August 17, 2021, T-Mobile released another statement , stating that "[while] our investigation is still underway and we continue to learn additional details, we have now been able to confirm that the data stolen from our systems did include some personal information."[32]

123. Finally, on August 19, 2021, T-Mobile shared an "Updated Information Regarding Ongoing Investigation into Cyberattack" on its website, confirming that a "bad actor had compromised T-Mobile systems" and that while the "investigation is ongoing," T-Mobile was able to confirm that data had been accessed and stolen by a cybercriminal, and that the information stolen may include personal information.[33] This information was later updated.

---

[30] Joseph Cox, *T-Mobile Investigating Claims of Massive Customer Data Breach*, VICE, August 15, 2021, available at https://www.vice.com/en/article/akg8wg/tmobile-investigating-customer-data-breach-100-million (last accessed Sep. 7, 2021). Vice's reporters confirmed that the information came from T-Mobile servers and included, at a minimum, social security numbers, phone numbers, names, physical addresses, unique device identifiers like IMEI numbers, and driver's license information. *See also* Michael Hill, *The T-Mobile data breach: A timeline*, CSO Online, Aug. 27, 2021, available at *https://www.csoonline.com/article/3630093/the-t-mobile-data-breach-a-timeline.html* (last accessed Sep. 7, 2021).

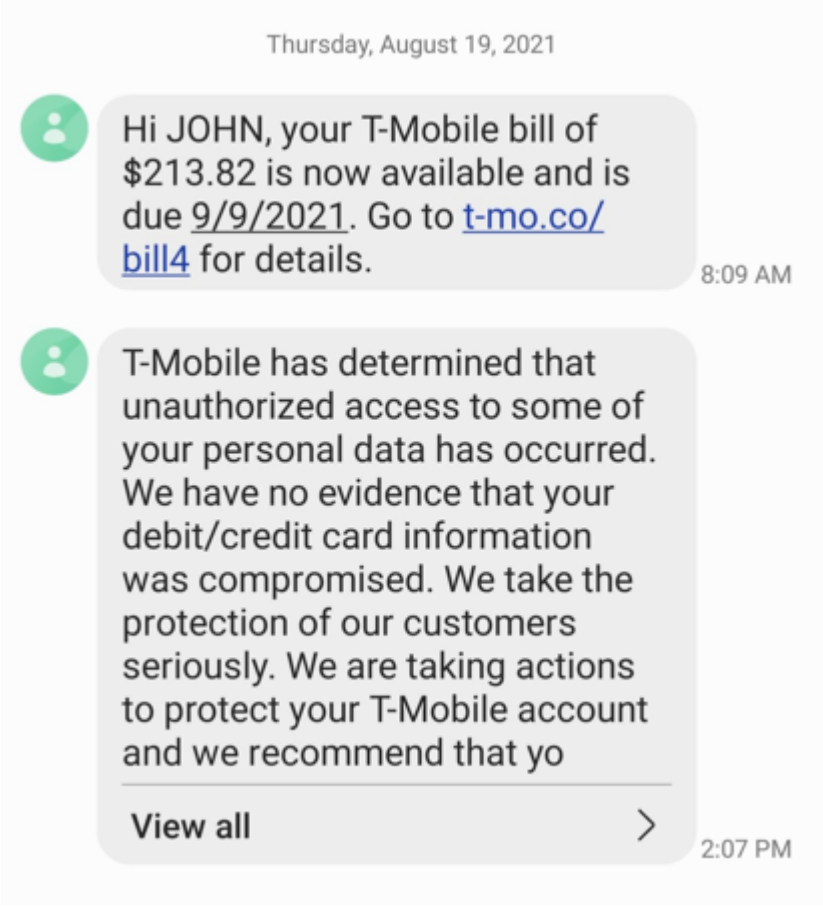
[31] Drew Fitzgerald, *T-Mobile Says Hackers Breached Company Database*, THE WALL STREET JOURNAL, August 16, 2021, available at https://www.wsj.com/articles/t-mobile-investigates-possible-data-breach-11629132916?mod=article_inline (last accessed Sep. 7, 2021).

[32] *T-Mobile Cybersecurity Incident Update*, Aug. 16, 2021, available at https://www.t-mobile.com/news/network/cybersecurity-incident-update-august-2021 (last accessed Sep. 7, 2021).

[33]

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

124. T-Mobile also began sending text messages to its customers, such as the one below received by Plaintiff John Precour:



125. T-Mobile's initial investigation revealed that "7.8 million current T-Mobile postpaid customer accounts' information appears to be contained in the stolen files, as well as just over 40 million records of former or prospective customers who had previously applied for credit with T-Mobile."[34]

126. As the investigation progressed, T-Mobile confirmed that for these 7.8 million postpaid customer accounts, the data stolen included "first and last names, date of birth, SSN, and driver's license/ID information" as well as "phone numbers" and "IMEI and IMSI information, the typical identifier numbers associated with a mobile phone."[35]

[34] Pedroja, *supra* n. 8.

[35] *T-Mobile Shares Updated Information Regarding Ongoing Investigation into Cyberattack*, August 20, 2021, available at https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation (last accessed Sep. 7, 2021).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

127. T-Mobile owed a duty to safeguard Plaintiffs' and class members' data based upon the promises that it made to its customers to safeguard data, as well as the disclosures that it made in its data security policies and privacy policies. T-Mobile voluntarily undertook efforts to keep that data secure as part of its business model and thus owes a continuing obligation to Plaintiffs and class members to keep their Private Information secure.

128. T-Mobile also owed a duty to comply with industry standards in safeguarding Private Information, which—as discussed herein—it did not do.

129. If T-Mobile had undertaken its data security obligations more seriously, particularly in light of the previous cybersecurity attacks it had suffered prior to this Data Breach, T-Mobile would have discovered and stopped the unauthorized access and extraction of private customer data.

130. The Data Breach was a targeted attack: T-Mobile was selected by Mr. Binns because it gathered PII from millions of present and former customers (like Plaintiff and Class Members), and was an easy target because its security level was "awful". Mr. Binns expected that he would be able to (and did) penetrate T-Mobile's defenses with rather rudimentary attacks and publicly available tools.[36]

131. There was no other apparent motivation for the extraction of this data, other than to profit from its sale.

132. T-Mobile has not indicated that Plaintiff and Class Members' stolen PII data was encrypted in any fashion, and upon information and belief, T-Mobile kept this data in unencrypted fields, ripe for the taking by even relatively unsophisticated hackers.

133. In response to exposing dozens of millions of individuals' PII, T-Mobile has provided a woefully inadequate recompense: twenty-four months of complimentary credit monitoring services. While this offer is a tacit acknowledgement by T-Mobile that Plaintiff and Class Members are now far more likely to suffer fraud and identity theft, this alone cannot make Plaintiff and Class Members whole.

[36] Fitzgerald and McMillan, *supra* n. 12.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

134. T-Mobile had an obligation created by contract, industry standards, common law, and representations made to its customers and even potential customers to keep their Private Information confidential, and to protect it from unauthorized access and disclosure.

135. Plaintiffs and Class Members provided their Private Information to T-Mobile with the reasonable expectation, and mutual understanding, that T-Mobile would comply with its obligations to keep such information confidential and secure from unauthorized access. This it failed to do.

C. T-Mobile Had Actual Knowledge of the Risk and Likelihood of a Data Breach of This Kind and Magnitude

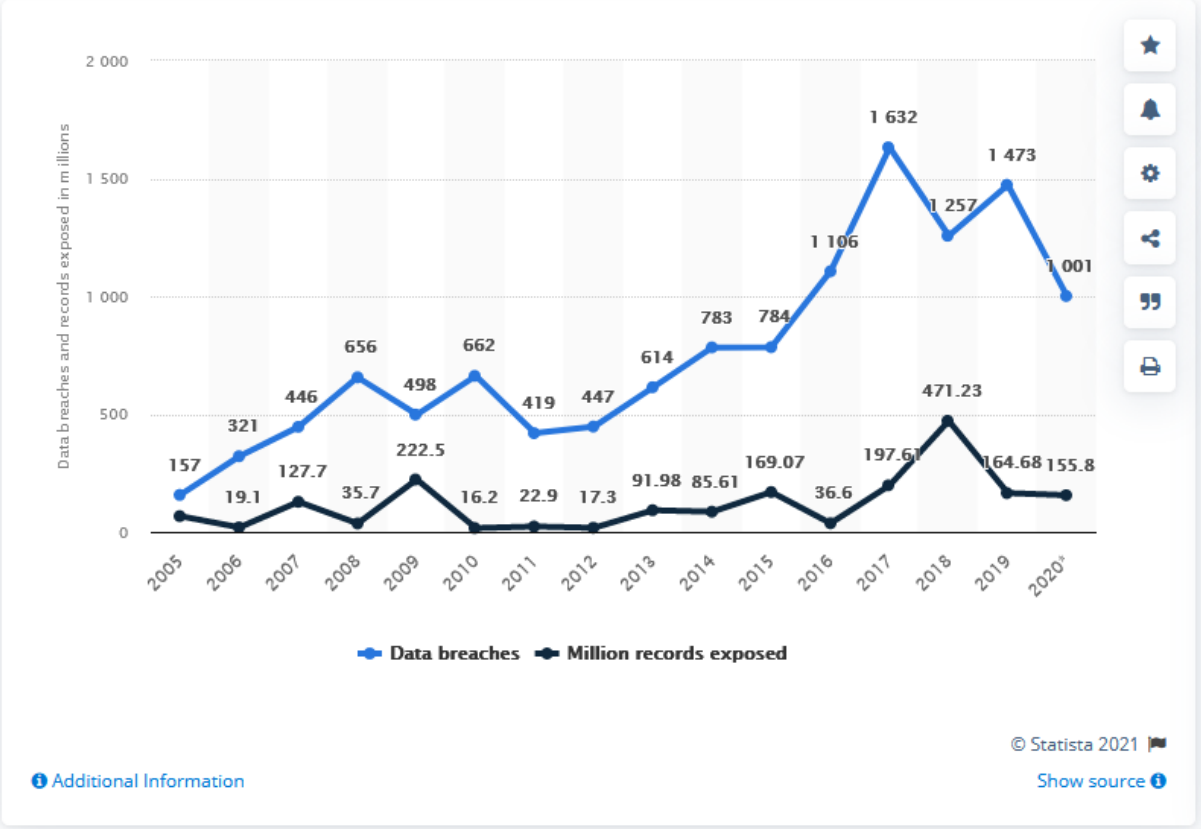
136. T-Mobile had actual knowledge of the risk and likelihood of cyberattacks on par with the one in this case, and acknowledged it in public filings and documents, because T-Mobile had suffered similar cyberattacks before.

137. Even if T-Mobile had not been the victim of four significant data breaches prior to this one, T-Mobile was aware of the increasing volume of cyberattacks and data breaches in its industry. For instance, Statista, a leading provider of market and consumer data, produced this graph entitled "Annual number of data breaches and exposed records in the United States from 2005 to 2020":[37]

[37] Available publicly at https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ (last accessed Sep. 7, 2021).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

138. T-Mobile should have been keenly aware that the nature of data collection and proliferation would increase the likelihood that the troves of PII that it kept would present an irresistible target to hackers.



139. T-Mobile appears to have understood this reality. In its 10-K Form, filed on December 31, 2020, that T-Mobile "expect[s] to continue to be the target of cyber-attacks, data breaches, or security incidents."[38]

140. However, T-Mobile failed to fully implement data security systems and protect critical Private Information belonging to consumers.

141. That Plaintiffs' and Class Members' PII was taken by hackers for the express purpose of identity theft and or sale to other criminals is not speculative: the manner in which T-Mobile learned about the Data Breach in the first place was because they were notified by an independent party that its customers data was being offered for sale.

[38] 2020 Form 10-K, at 12.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

142. Even worse, the fraudulent activity resulting from the Data Breach may not come to light for years: the kinds of data stolen are difficult to change and represent persistent data, data that bad actors may be able to use months or years later to commit identity theft and fraud.

143. T-Mobile knew, or reasonably should have known, of the importance of safeguarding the Private Information of Plaintiffs and Members of the Classes, including Social Security numbers, driver's license numbers, dates of birth, and device identifiers, and of the foreseeable consequences that would occur if T-Mobile's networks were breached, including, specifically, the significant costs that would be imposed on Plaintiffs and Class Members as a result of a breach.

144. In order to avoid future identity theft and/or fraud, Plaintiffs and Class Members must be constantly vigilant regarding their financial and personal accounts, and must expend additional time and money to secure their own identities. These mitigation damages are separate and distinct from the actual fraud or identity theft that many may suffer.

145. T-Mobile's failure to take reasonable, adequate steps to protect the PII of its customers, and past and potential future customers, was the direct and proximate cause of these injuries.

D. T-Mobile Failed to Comply with Industry and Regulatory Standards

146. Because of the value of PII and PHI to hackers and identity thieves, companies in the business of storing, maintaining and securing Private Information, such as T-Mobile, have been identified as being particularly vulnerable to cyber-attacks. Cybersecurity firms have promulgated a series of best practices that at minimum should be implemented by sector participants including, but not limited to: installing appropriate malware detection software; monitoring and limiting the network ports; protecting web browsers and email management systems; setting up network systems such as firewalls, switches and routers; monitoring and protection of physical security systems; protection against any possible communication system;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

and training staff regarding critical points.[39] Indeed, T-Mobile recognizes these best practices, and discusses many of them in its security and privacy protocols and policies.[40]

147. Additionally, part of a company's cybersecurity hygiene concerns the ability to patch software and ensure that older databases and servers remain secure.

148. Further, Federal and State governments have likewise established security standards and issued recommendations to diminish data breaches and the resulting harm to consumers and financial institutions. The FTC has issued numerous guides for business highlighting the importance of reasonable data and cyber security practices. According to the FTC, the need for data and cyber security should be factored into all business decision-making.[41]

149. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data and cyber security principles and practices for business.[42] The guidelines note businesses should protect the personal customer and consumer information that they keep; properly dispose of personal information that is no longer needed; encrypt information stored on computer networks; understand their network's vulnerabilities; and implement policies to correct security problems.[43] The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs; monitor all incoming traffic for activity indicating someone is attempting to hack the system; watch for large amounts of data being transmitted from the system; and have a response plan ready in the event of a breach.[44]

---

[39] *See White Paper: Addressing BPO Information Security: A Three-Front Approach*, DATAMARK, Inc. (Nov. 2016), https://insights.datamark.net/addressing-bpo-information-security/.
[40] T-Mobile Privacy Notice, https://www.t-mobile.com/privacy-center/our-practices/privacy-policy.
[41] *Start with Security: A Guide for Business* at 2, FTC (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf.
[42] *Protecting Personal Information: A Guide for Business*, FTC (Oct. 2016), https://www.ftc.gov/tips-advice/business-center/guidance/protecting-personal-information-guide-business.
[43] *See id.*
[44] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

150. The FTC recommends that companies not maintain cardholder information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity on the network; and verify that third-party service providers have implemented reasonable security measures.

151. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer and consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data and cyber security obligations.

152. T-Mobile also has obligations created by other federal and state law and regulations, contracts, industry standards, and common law to maintain reasonable and appropriate physical, administrative, and technical measures to keep Plaintiffs' and class members' Private Information confidential and to protect it from unauthorized access and disclosure.

153. T-Mobile was no stranger to following stringent security and privacy policies. Upon information and belief, as a government contractor under the Spiral 3 contract with the NAVSUP Headquarters at Navy base San Diego, as well as its participation in the GSA Schedule (also referred to as a Multiple Award Schedule and Federal Supply Schedule), which is a long-term, governmentwide contract with commercial firms providing federal, state, and local government buyers access to commercial products and services at volume discount prices, T-Mobile is subject to cyber security obligations stemming from federal law, such as the Privacy Act of 1974, as amended, 5 U.S.C. § 552a, and 48 C.F.R. § 52.204-21.[45]

[45] Darren Death, *Information Security Requirements for U.S. Federal Contractors*, Forbes (Sept. 4, 2018), https://www.forbes.com/sites/forbestechcouncil/2018/09/04/information-security-requirements-for-u-s-federal-contractors/#4c0c6b83451b.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

154. T-Mobile similarly violated other statutes by failing to implement reasonable security measures to mitigate the risk of unauthorized access, and encrypting necessary information.

155. Given the magnitude of the risk and repercussions of a breach or attack targeting this type of data, the likelihood of a breach or attack, and T-Mobile's explicit awareness of these vulnerabilities, T-Mobile should have taken every reasonable precaution in developing a robust security program and protecting Plaintiffs' and the class members' Private Information. However, T-Mobile failed to even employ appropriate safeguards, leaving the sensitive Private Information in its possession exposed to unauthorized access.

156. Despite its duties, representations, and promises, T-Mobile failed to adequately secure and protect its clients' data, including that of the numerous non-profits, such as the respective organizations which maintained Plaintiffs' and the class members' Private Information, allowing the Private Information to be accessed, disclosed, and misused.

E. T-Mobile's Failures Resulted in a Data Breach

157. Prior to the Data Breach, Plaintiffs and class members provided sensitive and PII to T-Mobile as required by T-Mobile to be considered for subscribership in its wireless plans. When providing such information, Plaintiffs and class members reasonably expected that the manager and securer of their Private Information, T-Mobile, would maintain security against cybercriminals and cyberattacks.

158. T-Mobile maintained Plaintiffs' and the class members' data on a shared network, server, and/or software. Despite its own awareness of steady increases of cyberattacks over the course of recent years, T-Mobile did not maintain adequate security of Plaintiffs' and the class members' Private Information and did not adequately protect it against hackers and cyberattacks.

159. T-Mobile maintained or abandoned login credentials on easily-accessed, unprotected routers that allowed access to servers on which T-Mobile kept Plaintiffs' and class members' Private Information.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

160. Upon information and belief, this sensitive PII was maintained on T-Mobile's servers in an unencrypted state.

161. T-Mobile breached its obligations to Plaintiffs and class members, and was otherwise negligent, wanton, and reckless, because it failed properly maintain and safeguard its networks and customer data. T-Mobile's unlawful conduct includes, but is not limited to, the following acts and/or omissions:

a. Failing to maintain an adequate data security system to reduce the risk of data breaches and cyber attacks;

b. Failing to adequately protect current, former, and prospective customers' Private Information;

c. Failing to properly monitor its own data security systems for intrusions;

d. Failing to comply with FTC guidelines for cybersecurity, in violation of Section 5 of the FTC Act, and;

e. Failing to adhere to industry standards for cybersecurity.

162. T-Mobile negligently and unlawfully failed to safeguard Plaintiffs' and class members' Private Information.

163. Accordingly, as outlined below, Plaintiffs and Class Members now face an increased risk of fraud and identity theft. In addition, Plaintiffs and Class Members also lost the benefit of the bargain they made with T-Mobile.

F. Data Breaches Put Consumers at Increased Risk of Fraud and Identify Theft

164. Private Information is valuable property. Its value is axiomatic, considering the market value and profitability of "Big Data" corporations in America. Illustratively, Alphabet Inc., the parent company of Google, reported in its 2020 Annual Report a total annual revenue of $182.5 billion and net income of $40.2 billion.[46] $160.7 billion of this revenue derived from

[46] Alphabet Inc., Annual Report (Form 10-K) at 32 (Feb. 3, 2021), https://www.sec.gov/ix?doc=/Archives/edgar/data/0001652044/000165204421000010/goog-20201231.htm.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

its Google business, which is driven almost exclusively by leveraging the Private Information it collects about the users of its various free products and services. America's largest corporations profit almost exclusively through the use of Private Information illustrating the considerable market value of personal Private Information.

165. Criminal law also recognizes the value of Private Information and the serious nature of the theft of such an asset by imposing prison sentences. This strong deterrence is necessary because cybercriminals earn significant revenue through stealing Private Information. Once a cybercriminal has unlawfully acquired personal data, the criminal can infinitely proliferate and use the information to commit fraud or identity theft, or sell the Private Information to another cybercriminal on a thriving black market.

166. Cybercriminals use conduct data breaches to make money and harm victims. Breaching large corporations' networks is a widely known and foreseeable threat in which a cybercriminal surreptitiously breaches a company's computer systems, and then locates and extracts valuable private and confidential information.

167. Once stolen, Private Information can be used in a number of different ways. One of the most common is that it is offered for sale on the "dark web," a heavily encrypted part of the Internet that makes it difficult for authorities to detect the location or owners of a website. The dark web is not indexed by normal search engines such as Google and is only accessible using a Tor browser (or similar tool), which aims to conceal users' identities and online activity. The dark web is notorious for hosting marketplaces selling illegal items such as weapons, drugs, and Private Information. Websites appear and disappear quickly, making it a dynamic environment.

168. The U.S. government, various U.S. and international law enforcement agencies, cybersecurity industry groups and laboratories, and numerous industry trade groups have issued warnings and guidance on managing and mitigating phishing and data breach threats. There are industry best practices for cybersecurity related to phishing and data breaches, some of which are particularly effective.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

169. For example, in 2019, both Microsoft and Google have publicly reported that using multi-factor authentication ("MFA") blocks more than 99% of automated hacks, including most ransomware attacks that occur because of unauthorized account access. Likewise, the reputable SANS Software Security Institute issued a paper stating "[t]ime to implement multi-factor authentication!"[47] An example of MFA implementation is receiving a text with a code when you input your username and password into a website; even if a cybercriminal knew your username and password, the cybercriminal would not be able to see the code on your phone and would thus be blocked from accessing your online account.

170. In this regard, implementing MFA "can block over 99.9 percent of account compromise attacks."[48]

171. The FBI concurs, listing "applying two-factor authentication wherever possible" as a best practice to defend against ransomware attacks.[49]

172. The industry that T-Mobile operates in has seen a substantial increase in cyberattacks and data breaches since as early as 2016.[50]

173. Indeed, cyberattacks have become so notorious that the FBI and Cybersecurity and Infrastructure Security Agency recently issued a warning to put potential targets on notice that they may be targeted for a potential attack.[51]

174. Cyberattacks and data breaches of cellular and wireless carriers are especially problematic because of the ubiquity with which most consumers use their phones: a smartphone is often the primary way by which an average consumer accesses their personal

---

[47] Matt Bromiley, *Bye Passwords: New Ways to Authenticate* at 3, SANS Software Security Inst. (July 2019), https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE3y9UJ.
[48] *What Is Multi-Factor Authentication (MFA)?*, Consensus Techs. (Sept. 16, 2020), https://www.concensus.com/what-is-multi-factor-authentication/#:~:text=The%20proof%20that%20MFA%20works,percent%20of%20account%20compromise%20attacks.
[49] *Ransomware Victims Urged to Report Infections to Federal Law Enforcement*, FBI (Sept. 15, 2016), https://www.ic3.gov/Media/Y2016/PSA160915.
[50] *Ransomware Victims Urged to Report Infections to Federal Law Enforcement*, FBI (Sept. 15, 2016), https://www.ic3.gov/Media/Y2016/PSA160915.
[51] Ben Kochman, *FBI, Cyber Officials Warn Of Labor Day Ransomware Push*, LAW360, Sep. 1, 2021, available at https://www.law360.com/insurance-authority/specialty-lines/articles/1418191/fbi-cyber-officials-warn-of-labor-day-ransomware-push (last accessed Sep. 7, 2021).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

and business email accounts, banking and financial accounts, local, state and federal government services, and maintain other confidential, personally identifying information.

175. The U.S. Government Accountability Office ("GAO") released a report in 2007 regarding data breaches finding that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[52]

176. The FTC recommends that identity theft victims take several steps to protect their personal health and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (and to consider an extended fraud alert that lasts for seven years if identity theft occurs), reviewing their credit reports, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.[53]

177. Cybercriminals use stolen Private Information such as SSNs for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank/finance fraud.

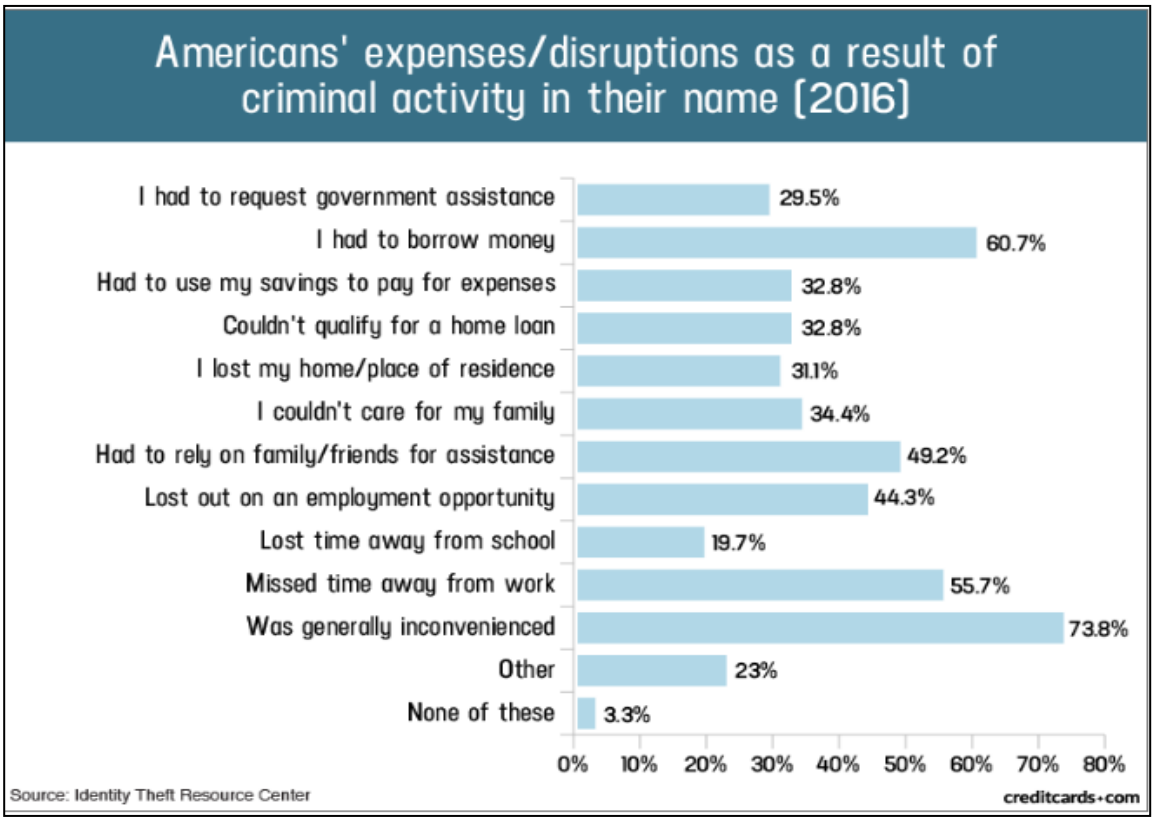
178. Identity thieves can also use SSNs to obtain a driver's license or other official identification card in the victim's name, but with the thief's picture; use the victim's name and SSN to obtain government benefits; or file a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house or receive medical services in the victim's name, seek unemployment or other benefits, and may even give the victim's Private Information to police during an arrest resulting in an arrest warrant being issued in the victim's name. A study by the Identity Theft Resource Center ("ITRC") shows the multitude of harms caused by fraudulent use of personal and financial information:

---

[52] *Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* ("GAO Report") at 2, GAO (June 2007), https://www.gao.gov/assets/270/262899.pdf.

[53] *Identity Theft Recovery Steps*, FTC, https://www.identitytheft.gov/Steps (last visited Mar. 23, 2021).

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992



[54]

179. As set forth above, 96.7% of study subjects experienced costs or other harms from the criminal activity.[55] As illustrated in the above graphic, this includes devastating results such as "I lost my home/place of residence" and "I couldn't care for my family." Moreover, the harms of identity theft are not limited to the affected individual and may adversely impact other associated persons and support systems, including government assistance programs. In the ITRC study, nearly one third of survey respondents had to request government assistance as a result of the identity theft, such as welfare, EBT, food stamps, or similar support systems.[56] The ITRC study concludes that "identity theft victimization has an

[54] Jason Steele, *Credit Card and ID Theft Statistics*, Creditcards.com (updated Oct. 24, 2017), https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php [https://web.archive.org/web/20171215215318/https://www.creditcards.com/credit-card-news/credit-card-security-id-theft-fraud-statistics-1276.php].
[55] *Id.*
[56] *Id.*

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

extreme and adverse effect on each individual as well as all of the support systems and people associated with the individual."[57]

180. Private Information is a valuable property right.[58] Its value is axiomatic, considering the value of Big Data in corporate America as well as the consequences of cyber thefts resulting in heavy prison sentences. This obvious risk to reward analysis illustrates that Private Information has considerable market value that is diminished when it is compromised.

181. It must also be noted there may be a substantial time lag—measured in years—between when harm occurs versus when it is discovered, and also between when Private Information and/or financial information is stolen and when it is used. According to the GAO, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[59]

Private Information is such an inherently valuable commodity to identity thieves that, once it compromised, criminals often trade the information on the cyber black-market for years.

182. There is a strong probability that entire batches of stolen information from the Data Breach have yet to be made available on the black market, meaning Plaintiffs and the class members are at an increased risk of fraud and identity theft for many years into the future. Thus, as the respective Notices advise, Plaintiffs must vigilantly monitor their financial accounts for many years to come.

VI. PLAINTIFFS' AND CLASS MEMBERS' INJURIES AND DAMAGES

183. Plaintiffs and class members have been harmed and incurred damages as a result of the compromise of their Private Information in the Data Breach. Plaintiffs' Private Information was compromised as a direct and proximate result of the Data Breach.

---

[57] *Id.*

[58] *See, e.g.*, John T. Soma et al., *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 Rich. J.L. & Tech. 11, at *1 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.").

[59] GAO Report, *supra* n. 52, at 29.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

A. Plaintiffs' and Class Members' Private Information was Compromised in the Data Breach

184. This security incident is not limited to automated attacks against the availability of information in T-Mobile's possession, custody or control. This incident included *unauthorized persons taking possession of the information*, available for their use however and whenever they see fit.

185. Plaintiffs include current customers of T-Mobile, as well as previous customers of T-Mobile and potential customers of T-Mobile. Plaintiffs were required to provide Private Information that was obtained and maintained by T-Mobile, which T-Mobile had a duty to secure and safeguard.

186. Like Plaintiffs, the class members' Private Information was compromised as a direct and proximate result of the Data Breach.

187. As a direct and proximate result of T-Mobile's conduct, Plaintiffs and the class members have been damaged because of the disclosure of their Private Information in several ways.

188. First, because there is already evidence of Plaintiffs' Private Information being offered for sale on the Internet, the stolen data clearly has value.

189. The risk borne by Plaintiffs and class members is a real one, evidenced by the notices received by the Plaintiffs, which continue to advise Plaintiffs to remain vigilant, monitor their credit, and engage in preventative measures to avoid identity theft.

190. Second, Plaintiffs and class members have sustained injuries as a result of the disclosure of their Private Information to unauthorized third-party cybercriminals as a result of T-Mobile's insufficient cybersecurity.

191. Plaintiffs have lost the value of their Private Information because the information is a valuable commodity. As discussed herein, T-Mobile demonstrated its value when it paid a ransom to avoid its disclosure. The cybercriminals also recognize its value—placing a price on what it would cost to acquire that information.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

192. Plaintiffs face real, concrete, and cognizable injuries as a result of the Data Breach, because cybercriminals confirmed that they exfiltrated data from T-Mobile's systems, there is no guarantee that the initial attempted sale of that information will be the only, or the last. As a result, Plaintiffs and class members must continue to be ever-vigilant to prevent identity theft and fraud from occurring as a result of the Data Breach.

193. As a result, Plaintiffs and class members face immediate and substantial risk of identity theft or fraud, such as loans opened in their names, medical services billed in their names, tax return fraud, utility bills opened in their names, credit card fraud, and similar identity theft.

194. In addition, because phone numbers and device identifiers were included in the Private Information, Plaintiffs are at substantial risk of having their phone numbers "ported", or used for spear-phishing scams.

195. Plaintiffs and the class members also face substantial risk of being targeted for future phishing, data intrusion, and other illegal schemes based on their Private Information as potential fraudsters could use that information to more effectively target such schemes to Plaintiffs.

196. Further, T-Mobile has not provided sufficient information to allow Plaintiffs and class members to adequately protect themselves. As a direct and proximate result of T-Mobile's conduct, Plaintiffs and the class members have and will continue to incur out-of-pocket costs for protective measures such as on-going credit monitoring fees and may also incur additional costs for credit report fees, and similar costs directly related to the Data Breach.

197. Plaintiffs and the class members have suffered or will suffer actual injury as a direct result of the Data Breach. Plaintiffs and the class members have and will suffer ascertainable losses in the form of out-of-pocket expenses and/or the loss of the value of their time spent in reasonably acting to remedy or mitigate the effects of the Data Breach relating to:

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

a. Finding fraudulent charges;

b. Canceling and reissuing credit and debit cards;

c. Addressing their inability to withdraw funds linked to compromised accounts;

d. Taking trips to banks and waiting in line to obtain funds held in limited accounts;

e. Placing "freezes" and "alerts" with credit reporting agencies;

f. Spending time on the phone with or at a financial institution to dispute fraudulent charges;

g. Contacting financial institutions and closing or modifying financial accounts;

h. Resetting automatic billing and payment instructions from compromised credit and debit cards to new ones;

i. Paying late fees and declined payment fees imposed as a result of failed automatic payments that were tied to compromised cards that had to be cancelled;

j. Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come; and

k. Interacting with government agencies and law enforcement to address the impact and harm caused by this breach.

198. Further, Plaintiffs and class members will have to continue to spend significant amounts of time to respond to the Data Breach and monitor their financial, student, and medical accounts and records for misuse.

199. Third, Plaintiffs have, at the very least, sustained nominal damages for T-Mobile's violations as discussed herein. As a result of T-Mobile's failures to safeguard Plaintiffs' and the class members' Private Information, they are forced to live with the knowledge that their Private Information—which contains private and personal details of their

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

life—may be disclosed to the entire world, thereby making them vulnerable to cybercriminals, permanently subjecting them to loss of security, and depriving Plaintiffs and the class members of their fundamental right to privacy.

200. Fourth, Plaintiffs are entitled to statutory damages, as provided, based upon the relevant claims alleged herein, and described below.

201. Fifth, T-Mobile was unjustly enriched at the expense of, and to the detriment of, Plaintiffs and class members. Among other things, T-Mobile continues to benefit and profit from class members' Private Information while its value to Plaintiffs and Class and Subclasses members has been diminished.

202. Finally, Plaintiffs and the class members have an interest in ensuring that their Private Information, which remains in the possession of T-Mobile, is protected from further breaches by the implementation of security measures and safeguards, including, but not limited to, making sure that the storage of data or documents containing Plaintiffs' and the class members' data is not accessible online and that access to such data is limited and secured.

VII. CLASS ACTION ALLEGATIONS

203. Plaintiffs bring this action on their own behalf and on behalf of all natural persons similarly situated, as referred to throughout this Complaint as "class members."

204. Pursuant to Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiffs propose the following Nationwide Class and Subclass definitions, subject to amendment as appropriate:

> **Nationwide Class:** All natural persons residing in the United States whose Personally Identifiable Information was compromised as a result of the Data Breach.

205. Federal Rules of Civil Procedure 23(b)(2) and (b)(3), Plaintiffs propose the following state-by-state claims in the alternative to the nationwide claims, as well as statutory claims brought under state data breach and consumer protection statutes, on behalf of statewide subclasses for each State, the District of Columbia, Puerto Rico, and the Virgin Islands (the "Statewide Subclasses"), subject to amendment as appropriate:

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

[State] Subclass: All natural persons residing in the [name of state or territory] whose Personally Identifiable Information was compromised as a result of the Data Breach.

206. Excluded from the Class and Subclasses are T-Mobile's officers, directors, and employees; any entity in which T-Mobile has a controlling interest; and the affiliates, legal representatives, attorneys, successors, heirs, and assigns of T-Mobile. Excluded also from the Class and Subclasses are members of the judiciary to whom this case is assigned, their families and members of their staff.

207. **Numerosity under Federal Rule of Civil Procedure 23(a)(1).** The members of the Class are so numerous and geographically dispersed that individual joinder of all class members is impracticable. While the exact number of class members is unknown to Plaintiffs at this time, based on information and belief, the class consists of at least 50 million present and former contract T-Mobile subscribers, prepaid T-Mobile subscribers, and potential subscribers to T-Mobile, whose data was compromised in the Data Breach, who can be identified by reviewing the Private Information exfiltrated from T-Mobile's databases.

208. **Commonality under Federal Rule of Civil Procedure 23(a)(2).** There are questions of law and fact common to Plaintiffs and class members, which predominate over any questions affecting only individual class members. These common questions of law and fact include, without limitation:

a. Whether T-Mobile unlawfully used, maintained, lost, or disclosed Plaintiffs' and the class members' Private Information;

b. Whether T-Mobile failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the Private Information compromised in the Data Breach;

c. Whether T-Mobile truthfully represented the nature of its security systems, including their vulnerability to hackers;

d. Whether T-Mobile's data security programs prior to and during the Data Breach complied with applicable data security laws and regulations;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

e. Whether T-Mobile's data security programs prior to and during the Data Breach were consistent with industry standards;

f. Whether T-Mobile owed a duty to class members to safeguard their Private Information;

g. Whether T-Mobile breached its duty to class members to safeguard their Private Information;

h. Whether cyberhackers obtained, sold, copied, stored or released class members' Private Information;

i. Whether T-Mobile knew or should have known that its data security programs and monitoring processes were deficient;

j. Whether the class members suffered legally cognizable damages as a result of T-Mobile's misconduct;

k. Whether T-Mobile's conduct was negligent;

l. Whether T-Mobile's conduct was negligent *per se*;

m. Whether T-Mobile's acts, inactions, and practices complained of herein amount to acts of intrusion upon seclusion under the law;

n. Whether T-Mobile failed to provide accurate and complete notice of the Data Breach in a timely manner; and

o. Whether the class members are entitled to damages, treble damages, civil penalties, punitive damages, and/or injunctive relief.

209. **Typicality under Federal Rule of Civil Procedure 23(a)(3).** Plaintiffs' claims are typical of those of the class members because Plaintiffs' Private Information, like that of every class member, was compromised in the Data Breach.

210. **Adequacy of Representation under Federal Rule of Civil Procedure (a)(4).** Plaintiffs will fairly and adequately represent and protect the interests of class members, including those from states and jurisdictions where they may not reside. Plaintiffs' Counsel are

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

competent and experienced in litigating class actions and were appointed to lead this litigation by the Court pursuant to Federal Rule of Civil Procedure 23(g).

211. **Predominance under Federal Rule of Civil Procedure 23(b)(3).** T-Mobile has engaged in a common course of conduct toward Plaintiffs and the class members, in that all Plaintiffs' and the class members' data at issue here was stored by T-Mobile and accessed during the Data Breach. The common issues arising from T-Mobile's conduct affecting class members, as described *supra*, predominate over any individualized issues. Adjudication of the common issues in a single action has important and desirable advantages of judicial economy.

212. **Superiority under Federal Rule of Civil Procedure 23(b)(3).** A class action is superior to other available methods for the fair and efficient adjudication of this controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Absent a class action, most class members would find that the cost of litigating their individual claim is prohibitively high and would therefore have no effective remedy. The prosecution of separate actions by individual class members would create a risk of inconsistent or varying adjudications with respect to individual class members, which would establish incompatible standards of conduct for T-Mobile. In contrast, the conduct of this action as a class action presents far fewer management difficulties, conserves judicial resources and the parties' resources, and protects the rights of each Class member.

213. **Injunctive Relief is Appropriate under Federal Rule of Civil Procedure 23(b)(2).** T-Mobile has failed to take actions to safeguard Plaintiffs' and class members' Private Information such that injunctive relief is appropriate and necessary. T-Mobile has acted on grounds that apply generally to the Class (and Subclasses) as a whole, so that class certification, injunctive relief, and corresponding declaratory relief are appropriate on a class-wide basis.

214. **Issue Certification Appropriate under Federal Rule of Civil Procedure 23(c)(4).** In the alternative, this litigation can be brought and maintained a class action with respect to particular issues, such as T-Mobile's liability with respect to the foregoing claims.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

215. Plaintiffs bring these claims on behalf of the Nationwide Class and Subclasses, as defined herein. The application of one specific state's laws to any cause of action is premature at this juncture, without the benefit of discovery, as T-Mobile maintained and maintains servers in several states.

216. Plaintiffs allege claims under the laws of individuals in all 50 states and territories because, based upon information and belief and the reasonable investigation of counsel given the limited information made available by T-Mobile concerning the Data Breach, individuals from all jurisdictions suffered injuries as a direct and proximate result of the Data Breach. Plaintiffs have standing to represent individuals in every jurisdiction, as described herein. To force Plaintiffs to search for specific, named representatives for all states at this stage in the litigation serves no useful purpose. See, e.g., In re Equifax, Inc., Customer Data Security Breach Litig., 362 F. Supp. 3d 1295, 1344 (N.D. Ga. 2019); In re Target Corp. Data Security Breach Litig., 66 F. Supp. 3d 1154, 1160 (D. Minn. 2014).

VIII. CLAIMS ON BEHALF OF THE NATIONWIDE CLASS

COUNT 1: NEGLIGENCE
(On Behalf of the Nationwide Class, or, Alternatively, on behalf of Plaintiffs and the Subclasses)

217. Plaintiffs identified above ("Plaintiffs," for purposes of these Counts), individually and on behalf of the Nationwide Class, repeat and allege Paragraphs 1-204, as if fully alleged herein. This claim is brought individually under the laws of the United States and all relevant State laws, on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding customer records.

218. T-Mobile owed Plaintiffs and class members a duty to exercise reasonable care in protecting their Private Information from unauthorized access or theft. T-Mobile breached

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

its duty of care by failing to implement reasonable security procedures and practices to protect this PII. Among other things, T-Mobile failed to:

a. implement security systems and practices consistent with federal and state guidelines;

b. implement security systems and practices consistent with industry norms;

c. timely detect the Data Breach; and

d. timely disclose the Data Breach to impacted customers.

219. T-Mobile knew or should have known that Plaintiffs' and class members' Private Information was highly sought after by cyber criminals and that Plaintiffs and class members would suffer significant harm if their Private Information was stolen by hackers.

220. T-Mobile knew, or should have known, that timely detection and disclosure of the Data Breach was required and necessary to allow Plaintiffs and class members to take appropriate actions to mitigate the resulting harm. These efforts include, but are not limited to, freezing accounts, changing passwords, monitoring credit scores/profiles for fraudulent charges, contacting financial institutions, and cancelling or monitoring government-issued IDs such as passports and driver's licenses.

221. T-Mobile had a special relationship with Plaintiffs and class members, because those Plaintiffs and class members entrusted T-Mobile with several different forms of Private Information. T-Mobile's customers were required to provide Private Information when purchasing or attempting to purchase T-Mobile's products and services. T-Mobile led Plaintiffs and class members to believe that it would take reasonable precautions to protect their Private Information and would timely inform them if their Private Information was compromised, which T-Mobile failed to do.

222. It was reasonably foreseeable that T-Mobile's breach of its duty of care would result in the injuries that Plaintiffs and class members suffered (and continue to suffer). T-Mobile failed to enact reasonable security procedures and practices, and as a result Plaintiffs and class members were the foreseeable victims of data theft that exploited the inadequate

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

security measures. The PII accessed in the Data Breach is precisely the type of information that cyber criminals seek and use to commit cyber crimes, and upon information and belief, was directly targeted by the hacker(s) in this case.

223. But-for T-Mobile's breach of its duty of care, the Data Breach would not have occurred and Plaintiffs' and class members' PII would not have been stolen and offered for sale by an unauthorized and malicious party.

224. As a direct and proximate result of T-Mobile's negligence, Plaintiffs and class members have been injured and are entitled to damages in an amount to be proven at trial. Such damages include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of the stolen Private Information; illegal sale of the compromised Private Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of their Private Information; lost value of unauthorized access to their Private Information; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

COUNT 2: NEGLIGENCE *PER SE*
(On Behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of Plaintiffs and the Subclasses)

225. Plaintiffs repeat and allege all preceding paragraphs, as if fully alleged herein.

226. Section 5 of the FTC Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce" including, as interpreted and enforced by the FTC, the unfair act or practice by T-Mobile of failing to use reasonable measures to protect PII. Various FTC publications and orders also form the basis of T-Mobile's duty.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

227. Defendant violated Section 5 of the FTC Act (and similar state statutes) by failing to use reasonable measures to protect PII and not complying with industry standards. Defendant's conduct was particularly unreasonable given the nature and amount of PII obtained and stored and the foreseeable consequences of a data breach on Defendant's systems.

228. Defendant's violation of Section 5 of the FTC Act (and similar state statutes) constitutes negligence per se.

229. Class members are consumers within the class of persons section 5 of the FTC Act (and similar state statutes) were intended to protect.

230. Moreover, the harm that has occurred is the type of harm the FTC Act (and similar state statutes) was intended to guard against. The FTC routinely pursues enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, cause the same harm suffered by Plaintiffs and class members in this case.

231. As a direct and proximate result of the T-Mobile's negligence, Plaintiffs and class members have been injured and are entitled to damages in an amount to be proven at trial. Such damages include one or more of the following: ongoing, imminent, certainly impending threat of identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; actual identity theft crimes, fraud, and other misuse, resulting in monetary loss and economic harm; loss of the value of their privacy and the confidentiality of their stolen Private Information; lost value of unauthorized access to their Private Information; illegal sale of the compromised Private Information on the black market; mitigation expenses and time spent on credit monitoring, identity theft insurance, and credit freezes and unfreezes; time spent in response to the Data Breach reviewing bank statements, credit card statements, and credit reports; expenses and time spent initiating fraud alerts; decreased credit scores and ratings; lost work time; lost value of the Private Information; lost benefit of their bargains and overcharges for services; and other economic and non-economic harm.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

COUNT 3: GROSS NEGLIGENCE
(On Behalf of Plaintiffs and the Nationwide Class, Or, alternatively, on behalf of Plaintiffs and the Subclasses)

232. Plaintiffs repeat and allege all preceding paragraphs, as if fully alleged herein.

233. Plaintiffs were required to submit non-public Private Information in order to become customers of T-Mobile. T-Mobile had a duty to Plaintiffs to securely maintain the Private Information collected as promised and warranted.

234. However, T-Mobile maintained unencrypted Personal Information on certain programs and/or servers. T-Mobile also maintained login credentials on unsecured routers, which allowed the breach of its network systems.

235. T-Mobile knew this information was (a) unencrypted and thus subject to breach and misuse; (b) included highly sensitive Private Information; and (c) that some of the data was "at rest," meaning the data was not in transit and being actively used.

236. The failure to encrypt this "at rest" data containing highly sensitive Personal Information of former customers was particularly flagrant and egregious.

237. Moreover, there was no reasonable reason for retaining these records which contain highly sensitive Private Information, including SSNs, for individuals who are no longer T-Mobile customers.

238. By voluntarily accepting the duty to maintain and secure this data, T-Mobile had a duty of care to use reasonable means to secure and safeguard its computer systems to prevent disclosure of the information, and to safeguard the information from cyber theft.

239. T-Mobile's duty included a responsibility to implement systems and processes by which it could detect and prevent a breach of its security systems in an expeditious manner and to give prompt notice to those affected by a data breach.

240. T-Mobile owed a duty of care to Plaintiffs to provide data security consistent with industry standards and other requirements discussed herein, and to ensure that its systems and networks, and the personnel responsible for them, adequately protected and safeguarded Plaintiffs' Private Information.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

241. T-Mobile owed an additional duty to Plaintiffs to take measures to ensure that, *inter alia*:

a. all Private Information was encrypted and continued to be encrypted;

b. "at rest" data is deleted after a reasonable amount of time; and/or

c. Plaintiffs were notified that their "at rest," sensitive and unencrypted Private Information had continued to be stored.

242. T-Mobile's duty of care to use reasonable security measures arose as a result of the special relationship that existed between T-Mobile and Plaintiffs.

243. Pursuant to the FTC Act, 15 U.S.C. § 45, T-Mobile had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs and the class members' Private Information. Plaintiffs and the class members are the individuals whom the FTC Act is intended to protect.

244. T-Mobile's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because T-Mobile is bound by industry standards to protect confidential Private Information.

245. T-Mobile consciously failed to use reasonable measures to protect Plaintiffs and class members' data. The specific gross negligent acts and omissions committed by T-Mobile include, but are not limited to, the following:

l. Consciously failing to adopt, implement, and maintain adequate security measures to safeguard Plaintiffs and class members' Private Information;

m. Consciously failing to ensure all sensitive Personal Information was encrypted;

n. Consciously failing to ensure all "at rest" data was destroyed in a reasonable amount of time;

o. Consciously failing to adequately monitor the security of its networks and systems;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

p. Consciously failing to periodically ensure that its email system had plans in place to maintain reasonable data security safeguards;

q. Consciously allowing unauthorized access to class members' Private Information;

r. Consciously failing to detect in a timely manner that class members' Private Information had been compromised; and

s. Consciously failing to timely notify Plaintiffs and class members about the Data Breach so those put at risk could take timely and appropriate steps to mitigate the potential for identity theft and other damages.

246. It was foreseeable that T-Mobile's conscious failure to use reasonable measures to protect the Plaintiffs class members' Private Information would result in injury to the Plaintiffs and class members. Further, the breach of security was reasonably foreseeable given the known high frequency of data breaches.

247. It was therefore foreseeable that the conscious failure to adequately safeguard the Plaintiffs and class members' Private Information would result in one or more types of injuries to Plaintiffs and class members.

248. Plaintiffs and class members are entitled to compensatory and consequential damages suffered as a result of the Data Breach.

COUNT 4: UNJUST ENRICHMENT
(On Behalf of Plaintiffs and the Nationwide Class, Or, alternatively, on behalf of Plaintiffs and the Subclasses)

249. Plaintiffs repeat and allege all preceding paragraphs, as if fully alleged herein.

250. Plaintiffs and the Texas Class have an interest, both equitable and legal, in the Private Information about them that was collected, secured, and maintained by T-Mobile, and that was ultimately compromised in the Data Breach.

251. A financial benefit was conferred upon T-Mobile when Plaintiffs and the Class provided their Private Information to T-Mobile. T-Mobile was enriched when it was provided

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

the ability to retain, use, and profit from that information. T-Mobile understood, at the time it received this Private Information, that it was so benefitting.

252. The relationship between T-Mobile and Plaintiffs and the Class is not attenuated, as Plaintiffs and the Class had a reasonable expectation that the security of their information would be maintained when they provided their information to T-Mobile. Plaintiffs and the Class were induced to provide their Private Information in reliance on the fact that T-Mobile's stated data security measures were adequate.

253. T-Mobile also benefitted through its unjust conduct by selling its services for more than those services were worth to Plaintiffs and the Class, who would not have applied for or used T-Mobile wireless plans at all, or at the terms offered by T-Mobile, had they been aware that T-Mobile would fail to protect their Private Information.

254. T-Mobile also benefitted through its unjust conduct by retaining money that it should have used to provide adequate data security to protect Plaintiffs' and Class members' Private Information.

255. But for T-Mobile's willingness and commitment to properly and safely collect, maintain and secure the Plaintiffs' Private Information, that information would not have been transferred to and entrusted with T-Mobile.

256. As a result of T-Mobile's wrongful conduct as alleged in this Complaint (including among things its utter failure to employ adequate data security measures, its continued maintenance and use of the Private Information belonging to Plaintiffs and the Class without having adequate data security measures, and its other conduct facilitating the theft of that Private Information), T-Mobile has been unjustly enriched at the expense of, and to the detriment of, Plaintiffs and the Class. Among other things, T-Mobile continues to benefit and profit from the sale of the Private Information while its value to Plaintiffs and Class and Subclasses members has been diminished.

257. T-Mobile's unjust enrichment is traceable to, and resulted directly and proximately from, the conduct alleged herein, including the collection, maintenance, and

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

inadequate security of Plaintiffs and the Class's sensitive Private Information, while at the same time failing to maintain that information secure from unauthorized access and exfiltration by cyber criminals.

258. It would be unjust, inequitable, and unconscionable for T-Mobile to be permitted to retain the benefits it received, and is still receiving, from Plaintiffs and the Class in connection with the collection, maintenance and security of their Private Information. T-Mobile's retention of such benefits under circumstances making it inequitable to do so constitutes unjust enrichment.

259. The benefit conferred upon, received, and enjoyed by T-Mobile was not conferred officiously or gratuitously, and it would be inequitable and unjust for T-Mobile to retain the benefit.

260. T-Mobile is therefore liable to Plaintiffs and the Class for restitution in the amount of the benefit conferred on T-Mobile as a result of its wrongful conduct, including specifically the value to T-Mobile of the Private Information that was stolen in the Data Breach and the profits T-Mobile is receiving from the use and sale of that information.

COUNT 5: BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of Plaintiffs and the Subclasses)

261. Plaintiffs repeat and allege all preceding paragraphs, as if fully alleged herein.

262. Plaintiffs and Class members entered into an implied contract with T-Mobile when they sought or obtained services from T-Mobile, or otherwise provided Private Information to T-Mobile.

263. As part of these transactions, T-Mobile agreed to safeguard and protect the Private Information of Plaintiffs and Class members.

264. Plaintiffs and Class members entered into implied contracts with the reasonable expectation that T-Mobile's data security practices and policies were reasonable and consistent

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

with industry standards. Plaintiffs and Class members believed that T-Mobile would use part of the monies paid to T-Mobile under the implied contracts to fund adequate and reasonable data security practices.

265. Plaintiffs and Class members would not have provided and entrusted their Private Information to T-Mobile, or would have paid less for T-Mobile's services in the absence of the implied contract or implied terms between them and T-Mobile. The safeguarding of Plaintiff and the Class's Private Information was a critical component of the intent of the parties.

266. Plaintiffs and class members fully performed their obligations under the implied contracts with T-Mobile.

267. T-Mobile breached its implied contracts with Plaintiffs and class members to protect their PII when it

a. failed to have security protocols and measures in place to protect that information; and

b. disclosed that information to unauthorized third parties.

268. As a direct and proximate result of T-Mobile's breach of implied contract, Plaintiffs and Class members sustained actual losses and damages as described in detail above, including that they did not get the benefit of the bargain for which they paid and were overcharged by T-Mobile for its services.

COUNT 6: DECLARATORY JUDGMENT
(On Behalf of Plaintiffs and the Nationwide Class, or alternatively, on behalf of Plaintiffs and the Subclasses)

269. Plaintiffs repeat and allege all preceding paragraphs, as if fully alleged herein.

270. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Furthermore, the Court has broad authority to restrain acts, such as

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

271. An actual controversy has arisen in the wake of the Data Breach regarding its present and prospective common law and other duties to reasonably safeguard Plaintiffs and Class members' Private Information and whether T-Mobile is currently maintaining data security measures adequate to protect Plaintiffs and Class members from further, future data breaches that compromise their Private Information.

272. Plaintiffs and Class members allege that T-Mobile's data security measures remain inadequate and T-Mobile has not provided any evidence that it has remedied the failure that occurred in the Data Breach at issue or has remedied any other vulnerability from its failure to properly assess threats by cybercriminals.

273. Plaintiffs and Class members continue to suffer injury as a result of the compromise of their Private Information and remain at imminent risk that further compromises of their Private Information will occur in the future.

274. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

a. T-Mobile continues to owe a legal duty to secure consumers' Private Information and to timely notify consumers of a data breach under the common law, the FTC Act, and various state statutes;

b. T-Mobile owes a duty by virtue of its special relationship, understanding that it is safeguarding sensitive, Private Information, or that it has already acknowledged a responsibility to keep such information safe by virtue of security policies; and

c. T-Mobile continues to breach this legal duty by failing to employ reasonable measures to secure consumers' Private Information.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

275. The Court also should issue corresponding prospective injunctive relief requiring T-Mobile to employ adequate security protocols consistent with law and industry standards to protect consumers' Private Information.

276. If an injunction is not issued, Plaintiffs and Class members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at T-Mobile. The risk of another such breach is real, immediate, and substantial. If another breach at T-Mobile occurs (as it has in the past), Plaintiffs and the Class will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

277. The hardship to Plaintiffs and the Class if an injunction does not issue exceeds the hardship to T-Mobile if an injunction is issued. Among other things, if another massive data breach occurs at T-Mobile, Plaintiffs and the Class will likely be subjected to substantial identify theft and other damage (as they cannot elect to store their information with another company). On the other hand, the cost to T-Mobile of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and T-Mobile has a pre-existing legal obligation to employ such measures even in the absence of a data breach.

278. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by helping to prevent another data breach at T-Mobile (and presenting an example to other, similar wireless carriers), thus eliminating the additional injuries that would result to Plaintiffs and the millions of consumers whose Private Information would be further compromised and potentially encouraging better adherence to best cybersecurity best practices by similar companies.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

IX. CLAIMS ON BEHALF OF THE STATE SUBCLASSES

CLAIMS ON BEHALF OF THE CALIFORNIA SUBCLASS

COUNT 1: CALIFORNIA CUSTOMER RECORDS ACT, Cal. Civ. Code §§ 1798.80, *et seq.*

279. The California Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-204, as if fully alleged herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding customer records.

280. "[T]o ensure that Personal Information about California residents is protected," the California legislature enacted Cal. Civ. Code § 1798.81.5, which requires that any business that "owns, licenses, or maintains Personal Information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the Personal Information from unauthorized access, destruction, use, modification, or disclosure."

281. T-Mobile is a business that owns, maintains, and licenses "personal information", within the meaning of Cal. Civ. Code § 1798.81.5(d)(1), about Plaintiff and California Subclass members.

282. Businesses that own or license computerized data that includes personal information, including SSNs, are required to notify California residents when their personal information has been acquired (or is reasonably believed to have been acquired) by unauthorized persons in a data security breach "in the most expedient time possible and without unreasonable delay." Cal. Civ. Code § 1798.82. Among other requirements, the security breach notification must include "the types of Personal Information that were or are reasonably believed to have been the subject of the breach." Cal. Civ. Code § 1798.82. Id.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

283. T-Mobile is a business that owns or licenses computerized data that includes personal information as defined by Cal. Civ. Code § 1798.82(h).

284. Plaintiff and California Subclass members' Private Information includes "personal information" as covered by Cal. Civ. Code §§ 1798.81.5(d)(1), 1798.82(h).

285. Because T-Mobile reasonably believed that Plaintiff and California Subclass members' Private Information was acquired by unauthorized persons during the Data Breach, T-Mobile had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by Cal. Civ. Code § 1798.82.

286. By failing to disclose the Data Breach in a timely and accurate manner, T-Mobile violated Cal. Civ. Code § 1798.82.

287. As a direct and proximate result of T-Mobile's violations of the Cal. Civ. Code §§ 1798.81.5 and 1798.82, Plaintiff and California Subclass members suffered damages, as described above.

288. Plaintiff and California Subclass members seek relief under Cal. Civ. Code § 1798.84, including actual damages and injunctive relief.

COUNT 2: CALIFORNIA UNFAIR COMPETITION LAW,

Cal. Bus. & Prof. Code §§ 17200, *et seq.*

289. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-204, as if fully alleged herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding unfair competition.

290. T-Mobile is a "person" as defined by Cal. Bus. & Prof. Code §17201.

291. T-Mobile violated Cal. Bus. & Prof. Code §§ 17200, *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

292. T-Mobile's "unfair" and "deceptive" acts and practices include:

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

a. T-Mobile's failure to implement and maintain reasonable security measures to protect Plaintiff and California Subclass members' Private Information from unauthorized disclosure, release, data breaches, and theft, which was a direct and proximate cause of the Data Breach. T-Mobile failed to identify foreseeable security risks, remediate identified security risks, and adequately improve security following previous cybersecurity incidents. For example, T-Mobile failed to protect an exposed, vulnerable router which held login credentials, which made it trivial for a hacker to penetrate T-Mobile's systems. This conduct, with little if any utility, is unfair when weighed against the harm to Plaintiff and the California Subclass, whose Private Information has been compromised.

b. T-Mobile's failure to implement and maintain reasonable security measures, which was also contrary to legislatively-declared public policy that seeks to protect consumers' data and ensure that entities that are trusted with it use appropriate security measures. These policies are reflected in laws, including California's Consumer Legal Remedies Act ("CLRA"), Cal Civ. Code § 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, the Confidentiality of Medical Information Act ("CMIA"), Cal Civ. Code § 56.26(b), and California's Consumer Records Act, Cal. Civ. Code § 1798.81.5.

c. T-Mobile's failure to implement and maintain reasonable security measures also lead to substantial consumer injuries, as described above, that are not outweighed by any countervailing benefits to consumers or competition. Moreover, because consumers could not know of T-

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Mobile's inadequate security, consumers could not have reasonably avoided the harms that T-Mobile caused.

d. Engaging in unlawful business practices by violating Cal. Civ. Code § 1798.82.

293. T-Mobile has engaged in "unlawful" business practices by violating multiple laws, including the CCRA, Cal. Civ. Code §§ 1798.80, *et seq.*, the CLRA, Cal. Civ. Code §§ 1780, *et seq.*, 15 U.S.C. § 680, *et seq.*, the FTC Act, 15 U.S.C. § 45, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b).

294. T-Mobile's unlawful practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and California Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by the CLRA, Cal. Civ. Code § 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d., COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and California Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by the CLRA, Cal. Civ. Code § 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b);

f. Failing to timely and adequately notify the Plaintiffs, and California Subclass members of the Data Breach;

g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and California Subclass members' Private Information; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by the CLRA, Cal. Civ. Code § 1780, *et seq.*, the FTC Act, 15 U.S.C. § 45, the GLBA, 15 U.S.C. § 6801, *et seq.*, HIPAA, 42 U.S.C. § 1320d, COPPA, 15 U.S.C. §§ 6501-6505, and the CMIA, Cal. Civ. Code § 56.36(b).

295. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' Private Information.

296. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the California Subclass members, into believing that their Private Information was not exposed and misled Plaintiffs and the California Subclass members into believing they did not need to take actions to secure their identities.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

297. As a direct and proximate result of T-Mobile's unfair, unlawful, and fraudulent acts and practices, Plaintiffs and California Subclass members were injured and lost money or property, including monetary damages from fraud and identity theft, time and expenses related to monitoring their financial accounts for fraudulent activity, an increased, imminent risk of fraud and identity theft, and loss of value of their Private Information, including but not limited to the diminishment of their present and future property interest in their Private Information and the deprivation of the exclusive use of their Private Information.

298. T-Mobile acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs and California Subclass members' rights.

299. Plaintiffs and California Subclass members seek all monetary and non-monetary relief allowed by law, including restitution of all profits stemming from T-Mobile's unfair, unlawful, and fraudulent business practices or use of their Private Information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief.

COUNT 3: CALIFORNIA CONSUMER LEGAL REMEDIES ACT,

Cal. Civ. Code §§ 1750, *et seq.*

300. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-204, as if fully alleged herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer legal remedies.

301. The Consumers Legal Remedies Act, Cal. Civ. Code §§ 1750, *et seq.* ("CLRA") is a comprehensive statutory scheme that is to be liberally construed to protect consumers against unfair and deceptive business practices in connection with the conduct of businesses

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

providing goods, property or services to consumers primarily for personal, family, or household use.

302. T-Mobile is a "person" as defined by Civil Code §§ 1761(c) and 1770, and has provided "services" as defined by Civil Code §§ 1761(b) and 1770. Specifically, T-Mobile provides wireless services to customers, and requires that subscribers provide certain Private Information in order to open and maintain an account with T-Mobile.

303. As part of the services T-Mobile offers, T-Mobile touts its ongoing efforts to keep consumers' Private Information secure, including by ensuring ongoing compliance with legal privacy standards established both domestically and abroad, as recognized by T-Mobile's Privacy Center. Indeed, T-Mobile purports that "**With T-Mobile, you don't have to worry.** Our privacy principles mean you can trust us to do the right thing with your data."

304. Plaintiffs and the California Class are "consumers" as defined by Civil Code §§ 1761(d) and 1770, and have engaged in a "transaction" as defined by Civil Code §§ 1761(e) and 1770.

305. T-Mobile's acts and practices were intended to and did result in the sales of products and services to Plaintiff and the California Subclass members in violation of Civil Code § 1770, including:

a. Representing that goods or services have characteristics and benefits that they do not have;

b. Representing that goods or services are of a particular standard, quality, or grade when they were not;

c. Advertising goods or services with intent not to sell them as advertised; and

d. Representing that the subject of a transaction has been supplied in accordance with a previous representation when it has not.

306. Specifically, T-Mobile violated Civil Code § 1770, in the following ways:

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and California Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the CMIA, Cal. Civ. Code § 56.36(b), which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and California Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the CMIA, Cal. Civ. Code § 56.36(b);

f. Failing to timely and adequately notify the Plaintiffs and California Subclass members of the Data Breach;

g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and California Subclass members' Private Information; and

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and California Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and the CMIA, Cal. Civ. Code § 56.36(b).

307. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' Private Information.

308. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the California Subclass members, into believing that their Private Information was not exposed and misled Plaintiffs and the California Subclass members into believing they did not need to take actions to secure their identities.

309. Had T-Mobile disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, T-Mobile was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the California Subclass. T-Mobile accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because T-Mobile held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the California Subclass members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

310. As a direct and proximate result of T-Mobile's violations of California Civil Code § 1770, Plaintiffs and California Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

theft; and loss of value of their Private Information, including but not limited to the diminishment of their present and future property interest in their Private Information and the deprivation of the exclusive use of their Private Information.

311. Plaintiffs and the California Subclass have provided notice of their claims for damages to T-Mobile, in compliance with California Civil Code § 1782(a), on October 4, 2021.

312. Plaintiffs and the California Subclass seek all monetary and non-monetary relief allowed by law, including damages, an order enjoining the acts and practices described above, attorneys' fees, and costs under the CLRA.

COUNT 4: CALIFORNIA CONSUMER PRIVACY ACT,

Cal. Civ. Code §§ 1798.100, *et seq.*

313. The California Plaintiffs identified above ("Plaintiffs," for purposes of this Count), individually and on behalf of the California Subclass, repeats and alleges Paragraphs 1-204, as if fully alleged herein. This claim is brought individually under the laws of California and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer privacy.

314. Plaintiffs and California Subclass members are residents of California.

315. T-Mobile is a corporation that is organized or operated for the profit or financial benefit of its shareholders or other owners, with annual gross revenues over $45 billion.

316. T-Mobile is a business that collects consumers' personal information as defined by Cal. Civ. Code § 1798.140(e). Specifically, T-Mobile obtains, receives, or accesses consumers' personal information when customers use T-Mobile's products to maintain and process consumer data.

317. T-Mobile and its direct customers determine the purposes and means of processing consumers' personal information. T-Mobile uses consumers' personal data to provide services at customers' requests, as well as to develop, improve, and test T-Mobile's services.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

318. T-Mobile violated Section 1798.150 of the California Consumer Privacy Act by failing to prevent Plaintiffs and the California Subclass members' nonencrypted and nonredacted personal information from unauthorized access and exfiltration, theft, or disclosure as a result of T-Mobile's violation of its duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information.

319. T-Mobile knew or should have known that its data security practices were inadequate to secure California Subclass members' Private Information and that its inadequate data security practices gave rise to the risk of a data breach.

320. T-Mobile failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the Private Information it collected and stored.

321. The cybercriminals accessed "nonencrypted and unredacted personal information" as covered by Cal. Civ. Code § 1798.81.5(A)(1)(d), in the Data Breach.

322. Upon information and belief, Plaintiff and California Subclass members' Private Information accessed by the cybercriminals in the Data Breach includes "nonencrypted and unredacted personal information" as covered by Cal. Civ. Code § 1798.81.5(A)(1)(d).

323. Plaintiffs seek injunctive relief in the form of an order requiring T-Mobile to employ adequate security practices consistent with law and industry standards to protect the California Subclass members' Private Information, requiring T-Mobile to complete its investigation, and to issue an amended statement giving a detailed explanation that confirms, with reasonable certainty, what categories of data were stolen and accessed without the California Subclass members' authorization, along with an explanation of how the data breach occurred.

324. Plaintiffs and the California Subclass members seek statutory damages or actual damages, whichever is greater, pursuant to Cal. Civil Code § 1798.150(a)(1)(A).

325. As a direct and proximate result of T-Mobile's violations of the Cal. Civ. Code §§ 1798.150, Plaintiff and California Subclass members suffered damages, as described above.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

326. On September 9, 2020, counsel for Mamie Estes served written notice identifying T-Mobile's violations of Cal. Civil Code § 1798.150(a) and demanding the data breach be cured, pursuant to Cal. Civil Code § 1798.150(b). On September 11, 2020, counsel for Philip Eisen, Mamie Estes, Shawn Regan and Kassandre Clayton, respectively, did the same. Because T-Mobile has neither cured the noticed violation nor and provided the Plaintiffs with an express written statement that the violations have been cured and that no further violations shall occur, Plaintiff and the California Subclass seek statutory damages pursuant to Cal. Civil Code § 1798.150(a)(1)(A).

CLAIMS ON BEHALF OF THE NORTH CAROLINA SUBCLASS

COUNT 5: NORTH CAROLINA IDENTITY THEFT PROTECTION ACT, N.C. Gen. Stat. §§ 75-60, *et seq.*

327. The North Carolina Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Carolina Subclass, repeats and alleges Paragraphs 1-204, as if fully alleged herein. This claim is brought individually under the laws of North Carolina and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding identity theft.

328. T-Mobile is a business that owns or licenses computerized data that includes "Personal Information" within the meaning of N.C. Gen. Stat. § 75-61(1) and N.C. Gen. Stat. §75-65.

329. Plaintiff and North Carolina Subclass members are "consumers" as defined by N.C. Gen. Stat. § 75-61(2).

330. T-Mobile is required to accurately notify Plaintiff and North Carolina Subclass members if it discovers a security breach, or receives notice of a security breach (where

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

unencrypted and unredacted Private Information was accessed or acquired by unauthorized persons), without unreasonable delay under N.C. Gen. Stat. § 75-65.

331. Plaintiff's and North Carolina Subclass members' Private Information includes "Personal Information" as covered under N.C. Gen. Stat. § 75-61(10).

332. Because T-Mobile discovered a security breach and had notice of a security breach (where unencrypted and unredacted Private Information was accessed or acquired by unauthorized persons), T-Mobile had an obligation to disclose the Data Breach in a timely and accurate fashion as mandated by N.C. Gen. Stat. § 75-65.

333. By failing to disclose the Data Breach in a timely and accurate manner, T-Mobile violated N.C. Gen. Stat. § 75-65.

334. A violation of N.C. Gen. Stat. § 75-65 is an unlawful trade practice under N.C. Gen. Stat. § 75-1.1.

335. As a direct and proximate result of T-Mobile's violations of N.C. Gen. Stat. § 75-65, Plaintiff and North Carolina Subclass members suffered damages, as described above.

336. Plaintiff and North Carolina Subclass members seek relief under N.C. Gen. Stat. §§ 75-16 and 16.1, including treble damages and attorney's fees.

COUNT 6: NORTH CAROLINA UNFAIR TRADE PRACTICES ACT, N.C. Gen. Stat. Ann. §§ 75-1.1, *et seq.*

337. The North Carolina Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the North Carolina Subclass, repeats and alleges Paragraphs 1-204, as if fully alleged herein. This claim is brought individually under the laws of North Carolina and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding unfair trade practices.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

338. T-Mobile advertised, offered, or sold goods or services in North Carolina and engaged in trade or commerce directly or indirectly affecting the people of North Carolina, as defined by N.C. Gen. Stat. Ann. § 75-1.1(b).

339. T-Mobile engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of N.C. Gen. Stat. Ann. § 75-1.1, including:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and North Carolina Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

d. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

e. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Carolina Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

f. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and North Carolina Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

g. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Carolina Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

h. Failing to timely and adequately notify the Plaintiffs, and North Carolina Subclass members of the Data Breach;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

i. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

j. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and North Carolina Subclass members' Private Information; and

k. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and North Carolina Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45; and

l. Failing to properly notify Plaintiff and North Carolina Subclass of the Data Breach violation of the North Carolina Identity Theft Protection Act, N.C. Gen. Stat. § 75-65.

340. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' Private Information.

341. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the North Carolina Subclass members, that their Private Information was not exposed and misled Plaintiffs and the North Carolina Subclass members into believing they did not need to take actions to secure their identities.

342. T-Mobile intended to mislead Plaintiff and North Carolina Subclass members and induce them to rely on its misrepresentations and omissions.

343. Had T-Mobile disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, T-Mobile was trusted with sensitive and valuable Private Information

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

regarding millions of consumers, including Plaintiffs, the Class, and the North Carolina Subclass. T-Mobile accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because T-Mobile held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the North Carolina Subclass members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

344. T-Mobile acted intentionally, knowingly, and maliciously to violate North Carolina's Unfair Trade Practices Act, and recklessly disregarded Plaintiff and North Carolina Subclass members' rights.

345. As a direct and proximate result of T-Mobile's unfair and deceptive acts and practices, Plaintiff and North Carolina Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

346. T-Mobile's conduct as alleged herein was continuous, such that after the first violations of the provisions pled herein, each week that the violations continued constitute separate offenses pursuant to N.C. Gen. Stat. Ann. § 75-8.

347. Plaintiff and North Carolina Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

CLAIMS ON BEHALF OF THE PENNSYLVANIA SUBCLASS

COUNT 7: VIOLATION OF THE PENNSYLVANIA UNFAIR TRADE PRACTICES AND CONSUMER PROTECTION LAW, 73 P.S. §§ 201-1, *et seq.*

348. The Plaintiff(s) identified above ("Plaintiff(s)," for purposes of this Count), individually and on behalf of the Pennsylvania Subclass, repeats and alleges all preceding paragraphs as if fully alleged herein. This claim is brought individually under the laws of

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Pennsylvania and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding unfair trade practices and consumer protection.

349. T-Mobile is a "person," as meant by 73 P.S. § 201-2(2).

350. Plaintiff and Pennsylvania Subclass members purchased goods and/or services primarily for personal, family, and/or household purposes.

351. T-Mobile engaged in unfair methods of competition and unfair or deceptive acts or practices in the conduct of its trade and commerce in violation of 73 P.S. § 201-3, including the following:

a. Representing that its goods and services have characteristics, uses, benefits, and qualities that they do not have (73 P.S. § 201-2(4)(v));

b. Representing that its goods and services are of a particular standard or quality if they are another (73 P.S. § 201-2(4)(vii));

c. Advertising its goods and services with intent not to sell them as advertised (73 P.S. § 201-2(4)(ix)); and

d. Engaging in any other fraudulent or deceptive conduct with creates a likelihood of confusion or of misunderstanding (73 P.S. § 201-2(4)(xxi)).

352. T-Mobile's unfair or deceptive acts and practices include:

a. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Pennsylvania Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

b. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

c. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Pennsylvania Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45, which was a direct and proximate cause of the Data Breach;

d. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Pennsylvania Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

e. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Pennsylvania Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45;

f. Failing to timely and adequately notify the Plaintiffs and Pennsylvania Subclass members of the Data Breach;

g. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

h. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Pennsylvania Subclass members' Private Information; and

i. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Pennsylvania Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45.

353. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' Private Information.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

354. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Pennsylvania Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Pennsylvania Subclass members into believing they did not need to take actions to secure their identities.

355. T-Mobile intended to mislead Plaintiff and Pennsylvania Subclass members and induce them to rely on its misrepresentations and omissions.

356. Had T-Mobile disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, T-Mobile was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Pennsylvania Subclass. T-Mobile accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because T-Mobile held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Pennsylvania Subclass members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

357. T-Mobile acted intentionally, knowingly, willfully, wantonly, maliciously, and outrageously to violate Pennsylvania Unfair Trade Practices and Consumer Protection Law, and recklessly disregarded Plaintiff and Pennsylvania Subclass members' rights.

358. As a direct and proximate result of T-Mobile's unfair methods of competition and unfair or deceptive acts or practices and Plaintiff's and the Pennsylvania Subclass' reliance on them, Plaintiff and Pennsylvania Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

359. Plaintiff and Pennsylvania Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages or statutory damages of $100 (whichever is greater), treble damages, punitive damages, attorneys' fees and costs, and any additional relief the Court deems necessary or proper.

CLAIMS ON BEHALF OF THE TEXAS SUBCLASS

COUNT 8: VIOLATION OF THE TEXAS DECEPTIVE TRADE PRACTICES—CONSUMER PROTECTION ACT, Texas Bus. & Com. Code §§ 17.41, *et seq.*

360. The Texas Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Texas Subclass, repeats and alleges all preceding paragraphs as if fully alleged herein. This claim is brought individually under the laws of Texas and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding consumer protection.

361. T-Mobile is a "person," as defined by Tex. Bus. & Com. Code § 17.45(3).

362. Plaintiffs and the Texas Subclass members are "consumers," as defined by Tex. Bus. & Com. Code § 17.45(4).

363. T-Mobile advertised, offered, or sold goods or services in Texas and engaged in trade or commerce directly or indirectly affecting the people of Texas, as defined by Tex. Bus. & Com. Code § 17.45(6).

364. T-Mobile engaged in false, misleading, or deceptive acts and practices, in violation of Tex. Bus. & Com. Code § 17.46(b), including:

a. Representing that goods or services have sponsorship, approval, characteristics, ingredients, uses, benefits or quantities that they do not have;

b. Representing that goods or services are of a particular standard, quality or grade, if they are of another; and

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

c. Advertising goods or services with intent not to sell them as advertised.

365. T-Mobile's false, misleading, and deceptive acts and practices include:

d. Failing to implement and maintain reasonable security and privacy measures to protect Plaintiff and Texas Subclass members' Private Information, which was a direct and proximate cause of the Data Breach;

e. Failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, and adequately improve security and privacy measures following previous cybersecurity incidents, which was a direct and proximate cause of the Data Breach;

f. Failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Texas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Texas's data security statute, Tex. Bus. & Com. Code § 521.052, which was a direct and proximate cause of the Data Breach;

g. Misrepresenting that it would protect the privacy and confidentiality of Plaintiff and Texas Subclass members' Private Information, including by implementing and maintaining reasonable security measures;

h. Misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Texas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Texas's data security statute, Tex. Bus. & Com. Code § 521.052;

i. Failing to timely and adequately notify the Plaintiffs and Texas Subclass members of the Data Breach;

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

j. Misrepresenting that certain sensitive Personal Information was not accessed during the Data Breach, when it was;

k. Omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiff and Texas Subclass members' Private Information; and

l. Omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiff and Texas Subclass members' Private Information, including duties imposed by the FTC Act, 15 U.S.C. § 45 and Texas's data security statute, Tex. Bus. & Com. Code § 521.052.

366. T-Mobile intended to mislead Plaintiff and Texas Subclass members and induce them to rely on its misrepresentations and omissions.

367. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' Private Information.

368. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Texas Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Texas Subclass members into believing they did not need to take actions to secure their identities.

369. Had T-Mobile disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, T-Mobile was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Texas Subclass. T-

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

Mobile accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because T-Mobile held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Texas Subclass members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

370. T-Mobile had a duty to disclose the above facts due to the circumstances of this case, the sensitivity and extent of the Private Information in its possession, and the generally accepted professional standards in its industry. This duty arose because members of the public, including Plaintiffs and the Texas Subclass, repose a trust and confidence in T-Mobile. In addition, such a duty is implied by law due to the nature of the relationship between consumers, including Plaintiffs and the Texas Subclass, and T-Mobile because consumers are unable to fully protect their interests with regard to their data, and placed trust and confidence in T-Mobile.

371. T-Mobile's duty to disclose also arose from its:

m. Possession of exclusive knowledge regarding the security of the data in its systems;

n. Active concealment of the state of its security; and/or

o. Incomplete representations about the security and integrity of its computer and data systems, and its prior data breaches, while purposefully withholding material facts from Plaintiffs and the Texas Subclass that contradicted these representations.

372. T-Mobile engaged in unconscionable actions or courses of conduct, in violation of Tex. Bus. & Com. Code Ann. § 17.50(a)(3). T-Mobile engaged in acts or practices which, to

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

consumers' detriment, took advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree.

373. Consumers, including Plaintiffs and Texas Subclass members, lacked knowledge about deficiencies in T-Mobile's data security because this information was known exclusively by T-Mobile. Consumers also lacked the ability, experience, or capacity to secure the Private Information in T-Mobile's possession or to fully protect their interests with regard to their data. Plaintiffs and Texas Subclass members lack expertise in information security matters and do not have access to T-Mobile's systems in order to evaluate its security controls. T-Mobile took advantage of its special skill and access to Private Information to hide its inability to protect the security and confidentiality of Plaintiffs and Texas Subclass members' Private Information.

374. T-Mobile intended to take advantage of consumers' lack of knowledge, ability, experience, or capacity to a grossly unfair degree, with reckless disregard of the unfairness that would result. The unfairness resulting from T-Mobile's conduct is glaringly noticeable, flagrant, complete, and unmitigated. The Data Breach, which resulted from T-Mobile's unconscionable business acts and practices, exposed Plaintiffs and Texas Subclass members to a wholly unwarranted risk to the safety of their Private Information and the security of their identity or credit, and worked a substantial hardship on a significant and unprecedented number of consumers. Plaintiffs and Texas Subclass members cannot mitigate this unfairness because they cannot undo the data breach.

375. T-Mobile acted intentionally, knowingly, and maliciously to violate Texas's

376. Deceptive Trade Practices-Consumer Protection Act, and recklessly disregarded Plaintiff and Texas Subclass members' rights.

377. As a direct and proximate result of T-Mobile's unconscionable and deceptive acts or practices, Plaintiffs and Texas Subclass members have suffered and will continue to

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information. T-Mobile's unconscionable and deceptive acts or practices were a producing cause of Plaintiffs' and Texas Subclass members' injuries, ascertainable losses, economic damages, and non-economic damages, including their mental anguish.

378. T-Mobile's violations present a continuing risk to Plaintiffs and Texas Subclass members as well as to the general public.

379. Plaintiffs and the Texas Subclass seek all monetary and non-monetary relief allowed by law, including economic damages; damages for mental anguish; treble damages for each act committed intentionally or knowingly; court costs; reasonably and necessary attorneys' fees; injunctive relief; and any other relief which the court deems proper.

CLAIMS ON BEHALF OF THE VIRGINIA SUBCLASS

COUNT 7: VIRGINIA CONSUMER PROTECTION ACT,
Va. Code § 59.1-196 *et seq.*

380. The Virginia Plaintiff(s) identified above ("Plaintiff," for purposes of this Count), individually and on behalf of the Virginia Subclass, repeats and alleges Paragraphs 1-204, as if fully alleged herein. This claim is brought individually under the laws of Virginia and on behalf of all other natural persons whose Private Information was compromised as a result of the Data Breach and reside in states having similar laws regarding unfair trade practices.

381. T-Mobile advertised, offered, or sold goods or services in Virginia and engaged in trade or commerce directly or indirectly affecting the people of Virginia, as defined by Va. Code § § 59.1-198.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

382. T-Mobile engaged in unfair and deceptive acts and practices in or affecting commerce, in violation of Va. Code § 59.1-200, including:

a. Misrepresenting goods or services as those of another;

b. Misrepresenting the source, sponsorship, approval, or certification of goods or services;

c. Misrepresenting that goods or services have certain quantities, characteristics, ingredients, uses, or benefits;

d. Misrepresenting that goods or services are of a particular standard, quality, grade, style, or model;

e. Advertising goods or services with intent not to sell them as advertised, or with intent not to sell at the price or upon the terms advertised; or

f. Using any other deception, fraud, false pretense, false promise, or misrepresentation in connection with a consumer transaction.

383. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of T-Mobile's data security and ability to protect the confidentiality of consumers' Private Information.

384. T-Mobile's representations and omissions were material because they were likely to deceive reasonable consumers, including Plaintiffs and the Virginia Subclass members, that their Private Information was not exposed and misled Plaintiffs and the Virginia Subclass members into believing they did not need to take actions to secure their identities.

385. T-Mobile intended to mislead Plaintiff and Virginia Subclass members and induce them to rely on its misrepresentations and omissions.

386. Had T-Mobile disclosed to Plaintiffs and Class members that its data systems were not secure and, thus, vulnerable to attack, T-Mobile would have been unable to continue in

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

business and it would have been forced to adopt reasonable data security measures and comply with the law. Instead, T-Mobile was trusted with sensitive and valuable Private Information regarding millions of consumers, including Plaintiffs, the Class, and the Virginia Subclass. T-Mobile accepted the responsibility of being a steward of this data while keeping the inadequate state of its security controls secret from the public. Accordingly, because T-Mobile held itself out as maintaining a secure platform for Private Information data, Plaintiffs, the Class, and the Virginia Subclass members acted reasonably in relying on T-Mobile's misrepresentations and omissions, the truth of which they could not have discovered.

387. T-Mobile acted intentionally, knowingly, and maliciously to violate Virginia's Unfair Trade Practices Act, and recklessly disregarded Plaintiff and Virginia Subclass members' rights.

388. As a direct and proximate result of T-Mobile's unfair and deceptive acts and practices, Plaintiff and Virginia Subclass members have suffered and will continue to suffer injury, ascertainable losses of money or property, and monetary and non-monetary damages, including from fraud and identity theft; time and expenses related to monitoring their financial accounts for fraudulent activity; an increased, imminent risk of fraud and identity theft; and loss of value of their Private Information.

389. T-Mobile's conduct as alleged herein was continuous, such that after the first violations of the provisions pled herein, each week that the violations continued constitute separate offenses pursuant to N.C. Gen. Stat. Ann. § 75-8.

390. Plaintiff and Virginia Subclass members seek all monetary and non-monetary relief allowed by law, including actual damages, treble damages, and attorneys' fees and costs.

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

X. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray for judgment as follows:

A. For an Order certifying this action as a class action and appointing Plaintiff and their Counsel to represent the Class;

B. For equitable relief enjoining T-Mobile from engaging in the wrongful conduct complained of herein pertaining to the misuse and/or disclosure of Plaintiff's and the Class members' Private Information, and from refusing to issue prompt, complete and accurate disclosures to Plaintiff and the Class or to mitigate further harm;

C. For equitable relief compelling T-Mobile to utilize appropriate methods and policies with respect to consumer data collection, storage, and safety, and to disclose with specificity the type of Private Information compromised during the Data Breach;

D. For equitable relief requiring restitution and disgorgement of the revenues wrongfully retained as a result of T-Mobile's wrongful conduct;

E. For an award of actual damages, compensatory damages, statutory damages, and statutory penalties, in an amount to be determined, as allowable by law;

F. For an award of punitive damages, as allowable by law;

G. For an award of attorneys' fees and costs, and any other expense, including reasonable expert witness fees;

H. Pre- and post-judgment interest on any amounts awarded; and

I. Such other and further relief as this court may deem just and proper.

XI. JURY TRIAL DEMAND

Plaintiffs hereby demand a jury trial for all claims so triable.

Dated this 15th day of October, 2021

Respectfully submitted,

By: /s/ Kim D. Stephens
Kim D. Stephens, P.S., WSBA #11984
/s/ Jason T. Dennett
Jason T. Dennett, WSBA #30686
/s/ Kaleigh N. Powell
Kaleigh N. Powell, WSBA #52684

TOUSLEY BRAIN STEPHENS PLLC
1200 Fifth Avenue, Suite 1700
Seattle, Washington 98101
TEL. 206.682.5600 • FAX 206.682.2992

TOUSLEY BRAIN STEPHENS, PLLC
1200 Fifth Avenue, Suite 1700
Seattle, WA 98101
Tel: (206) 682-5600
Fax: (206) 682-2992
jdennett@tousley.com
kstephens@tousley.com
kpowell@tousley.com

Amy E. Keller*
James A. Ulwick*
DiCELLO LEVITT GUTZLER LLC
Ten North Dearborn Street, Sixth Floor
Chicago, IL 60602
Tel: (312) 214-7900
Fax: (312) 253-1443
akeller@dicellolevitt.com
julwick@dicellolevitt.com

William A. Kershaw
Ian J. Barlow
KERSHAW, COOK & TALLEY PC
401 Watt Avenue
Sacramento, CA 95846
Tel: (916) 779-7000
Fax: (916) 244-4829
bill@kctlegal.com
ian@kctlegal.com

Tyler H. Fox, Esq.
Law Offices of Tyler H. Fox
135 Antrim St.
Unit #2
Cambridge, MA 02139
Tel: (857) 260-3105
tylerfox@verizon.net

**Pro Hac Vice applications to follow*